

# User's Manual

## RadiNET<sup>®</sup> Pro Web Hosting

Network QC Management Server Provider

### **Important**

**Please read this User's Manual carefully to familiarize yourself with safe and effective usage.**



# About This Manual

This manual describes how to install and configure RadiNET Pro Gateway and RadiCS for connecting to RadiNET Pro Web Hosting. Read this manual together with the RadiNET Pro User's Manual, and then build and operate correctly.

"SYSTEM" (page 5)	"Chapter 1 Introduction" (page 6) "Chapter 2 About Group" (page 8) "Chapter 3 About Network Configuration" (page 10)
"SETUP" (page 12)	"Chapter 4 About Administrator Computer" (page 13) "Chapter 5 Setup of Gateway Computer" (page 15) "Chapter 6 Setup of RadiCS Computer (WORKGROUP)" (page 40) "Chapter 7 Setup of RadiCS Computer (DOMAIN)" (page 67)
"MAINTENANCE" (page 115)	"Chapter 8 Management of Gateway Computer" (page 116) "Chapter 9 About Log" (page 121)
"REFERENCE" (page 126)	"Chapter 10 About Security" (page 127) "Chapter 11 About License" (page 129) "Chapter 12 Other Settings" (page 133) "Chapter 13 Adding monitors" (page 137)

---

No part of this manual may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electric, mechanical, or otherwise, without the prior written permission of EIZO NANA O CORPORATION.

EIZO NANA O CORPORATION is under no obligation to hold any submitted material or information confidential unless prior arrangements are made pursuant to EIZO NANA O CORPORATION's receipt of said information. Although every effort has been made to ensure that this manual provides up-to-date information, please note that these product specifications are subject to change without notice.

---

Internet Explorer, Microsoft, Windows, Windows Vista, Windows Server, Internet Information Service (IIS), Active Directory and .NET Framework are registered trademarks of Microsoft Corporation in the United States and other countries.

Firefox is a registered trademark of the Mozilla Foundation.

EIZO, the EIZO Logo, RadiForce, RadiNET and RadiCS are registered trademarks of EIZO NANA O CORPORATION in Japan and other countries.

All other company and product names are trademarks or registered trademarks of their respective owners.

---

# CONTENTS

<b>Cover</b> .....	<b>1</b>		
<b>About This Manual</b> .....	<b>2</b>		
<b>CONTENTS</b> .....	<b>3</b>		
<b>SYSTEM</b> .....	<b>5</b>		
<b>Chapter 1 Introduction</b> .....	<b>6</b>		
1-1. Functional Overview of the System .....	6		
1-2. System Requirements .....	7		
● System Requirements for RadiNET Pro Gateway .....	7		
● System Requirements for Administrator Computer .....	7		
● System Requirements for RadiNET Pro Administrator Mobile devices .....	7		
<b>Chapter 2 About Group</b> .....	<b>8</b>		
2-1. Functional Overview of the Group .....	8		
● What is Group? .....	8		
2-2. Difference of the RadiNET Pro Gateway Authentication depending on the Group ...	9		
<b>Chapter 3 About Network Configuration</b> .....	<b>10</b>		
3-1. Network Configuration of the System .....	10		
● HTTPS Communications .....	10		
● Socket Communications .....	10		
3-2. Overview of the System Communication ..	11		
3-3. About Internet Connection .....	11		
<b>SETUP</b> .....	<b>12</b>		
<b>Chapter 4 About Administrator Computer</b> ...	<b>13</b>		
4-1. About Administrator Computer .....	13		
4-2. How to Use Management Console .....	13		
<b>Chapter 5 Setup of Gateway Computer</b> .....	<b>15</b>		
5-1. About Installation .....	15		
5-2. Preparing Management Group .....	16		
5-3. Installation of .NET Framework .....	18		
5-4. Installation of RadiNET Pro Gateway .....	20		
5-5. Connecting to Enterprise Server .....	24		
5-6. Changing the Query Interval .....	26		
5-7. Setting the Port Number for RadiNET Pro Gateway .....	28		
5-8. Installation of RadiCS Network Upgrade Software Server .....	30		
5-9. Setting the Port Number for RadiCS Network Upgrade Software .....	33		
5-10. Configuring Windows Firewall .....	34		
● For Windows XP / Vista / Server 2003 .....	34		
● Windows 7 / Server 2008 / 2008 R2 .....	36		
5-11. Confirmation of the RadiCS Network Upgrade Software Server Operation .....	39		
<b>Chapter 6 Setup of RadiCS Computer (WORKGROUP)</b> .....	<b>40</b>		
6-1. Setup of RadiCS Computer .....	41		
6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service .....	42		
6-3. Installation of RadiCS .....	45		
6-4. Installation of RadiCS Network Upgrade Software .....	49		
6-5. Configuring RadiCS Network Upgrade Software .....	51		
6-6. Configuring the Local Security Policy .....	54		
6-7. Configuring Windows Firewall .....	57		
● For Windows XP / Vista .....	57		
● For Windows 7 .....	59		
6-8. Connecting to RadiNET Pro Server .....	61		
6-9. Setting a user account for RadiCS Network Upgrade Software service .....	64		
<b>Chapter 7 Setup of RadiCS Computer (DOMAIN)</b> .....	<b>67</b>		
7-1. Setup of RadiCS Computer .....	68		
7-2. Creating “Organizational Unit” in Domain .....	69		
● For both Windows Server 2003 and Windows Server 2008 .....	69		
7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service .....	71		
● For both Windows Server 2003 and Windows Server 2008 .....	71		
7-4. Registering RadiCS Computer to “Organizational Unit” .....	75		
● For both Windows Server 2003 and Windows Server 2008 .....	75		
7-5. Setting of Group Policy .....	77		
● For Windows Server 2003 .....	77		
● For Windows Server 2008 .....	85		
7-6. Configuring Windows Firewall of RadiCS Computer by Group Policy .....	92		
● For Windows Server 2003 .....	92		
● Windows Server 2008 / 2008 R2 .....	96		
7-7. Installation of RadiCS .....	100		
7-8. Installation of RadiCS Network Upgrade Software .....	104		
7-9. Configuring RadiCS Network Upgrade Software .....	106		

7-10.	Connecting to RadiNET Pro Server .....	109
7-11.	Setting a user account for RadiCS Network Upgrade Software service.....	112
<b>MAINTENANCE .....</b>		<b>115</b>
<b>Chapter 8 Management of Gateway Com- puter .....</b>		<b>116</b>
8-1.	Changing the Number of Simultaneous Connections .....	116
8-2.	How to Change Gateway Computers.....	118
<b>Chapter 9 About Log .....</b>		<b>121</b>
9-1.	Remote Operation Log of Enterprise Server .....	121
9-2.	Remote Operation Log of Gateway Computer .....	122
9-3.	Remote Operation Log of RadiCS Computer .....	124
9-4.	About Other Logs .....	125
●	System Log of Enterprise Server .....	125
●	System Log of Gateway Computer .....	125
●	Error Log of RadiCS Computer.....	125
<b>REFERENCE .....</b>		<b>126</b>
<b>Chapter 10 About Security .....</b>		<b>127</b>
10-1.	Security of the System .....	127
10-2.	Identification and Authentication of User.....	127
10-3.	Identification and Authentication of Device.....	127
10-4.	Securing of Communication Path.....	127
10-5.	Recording Remote Operation Log .....	128
10-6.	Patient Information .....	128
<b>Chapter 11 About License .....</b>		<b>129</b>
11-1.	License Required for Gateway Computer.....	129
11-2.	License Required for SQL Server .....	131
<b>Chapter 12 Other Settings .....</b>		<b>133</b>
12-1.	Moving Monitors between Groups .....	133
12-2.	Access Restriction to Management Console .....	134
●	For Windows Server 2003 .....	134
●	For Windows Server 2008 .....	136
<b>Chapter 13 Adding monitors .....</b>		<b>137</b>
13-1.	Procedures on RadiCS Computer.....	137
13-2.	Procedures on RadiNET Pro Server .....	138

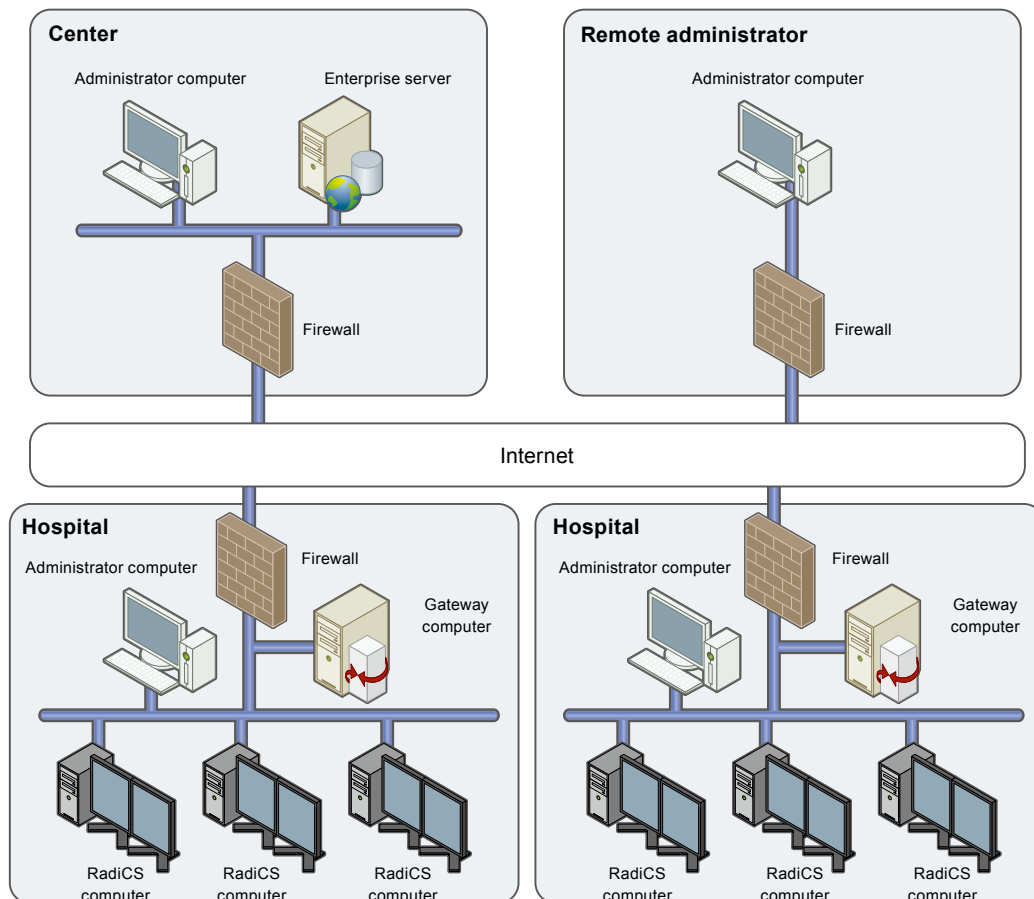
# SYSTEM

# Chapter 1 Introduction

## 1-1. Functional Overview of the System

RadiNET Pro Web Hosting is a system that allows you to use a Web browser to access Enterprise server from a networked administrator computer and manage the asset management and quality control of monitors.

### Functional Overview of the System



- Enterprise server: This is a server with RadiNET Pro Enterprise installed. EIZO NANO CORPORATION sets up and manages this server.
- Gateway computer: This is a computer with RadiNET Pro Gateway installed.
- RadiCS computer: This is a computer with RadiCS installed.
- Administrator computer: This is a computer that accesses the management console of Enterprise server.

- 1. Administrator computer can access Enterprise server, and then use the management console to check the quality management history of the monitor.**
- 2. According to the instruction from the administrator computer, Enterprise server manages the monitor connected to RadiCS computer.**
- 3. Various inspection results (monitor management history) of the RadiCS computer are sent to Enterprise server, and then stored in the database.**

## 1-2. System Requirements

### ● System Requirements for RadiNET Pro Gateway

Hardware	<p>CPU</p> <ul style="list-style-type: none"><li>• 3GHz Pentium 4 or more</li></ul> <p>For Windows Server 2008 R2, 64-bit (x64) processor 1.4GHz or higher is required</p> <p>Hard disk drive</p> <ul style="list-style-type: none"><li>• 50GB or more</li></ul> <p>Memory</p> <ul style="list-style-type: none"><li>• 1GB or more</li></ul>
OS	<ul style="list-style-type: none"><li>• Windows XP Professional SP3 (32bit)<sup>*1</sup> <sup>*2</sup></li><li>• Windows Vista SP2 (32bit)<sup>*1</sup> <sup>*2</sup></li><li>• Windows 7 SP1<sup>*2</sup></li><li>• Windows Server 2003 R2 Standard Edition SP2 (32bit)<sup>*1</sup> <sup>*3</sup></li><li>• Windows Server 2008 Standard SP2 (32bit)<sup>*1</sup> <sup>*3</sup></li><li>• Windows Server 2008 R2 Standard SP1<sup>*3</sup></li></ul>
Software	<ul style="list-style-type: none"><li>• RadiNET Pro Gateway Ver.4.1.0</li><li>• .NET Framework 4<sup>*4</sup></li><li>• Windows Installer 3.1<sup>*4</sup></li></ul>
	<ul style="list-style-type: none"><li>• Security software<ul style="list-style-type: none"><li>- Antivirus</li><li>- Firewall</li></ul></li></ul>
Other communication devices	<ul style="list-style-type: none"><li>• Devices including the following are required to set up an appropriate communication environment:<ul style="list-style-type: none"><li>- Router</li><li>- Firewall</li></ul></li></ul>

<sup>\*1</sup> Unsupporting 64-bit OS.

<sup>\*2</sup> If you use Windows XP, Windows Vista or Windows 7, conform the terms of the license before using.

<sup>\*3</sup> If you use Microsoft Windows Server 2003 /2008, the Client Access license (CAL) in accordance with Microsoft licensing is required. Refer to “[Chapter 11 About License](#)” ([page 129](#)) about CAL for details.

<sup>\*4</sup> Provided separately.

### ● System Requirements for Administrator Computer

Hardware	<p>Resolution: 1,280 x 1,024 or higher</p> <p>Color palette: 24 bits or more</p>
Software	<p>Internet Explorer 8.0, 9.0</p> <p>Firefox <sup>*1</sup></p> <p>Adobe Reader</p>

<sup>\*1</sup> A test has been performed with the latest version at the time of release.

### ● System Requirements for RadiNET Pro Administrator Mobile devices

Hardware	<p>Resolution: 320 x 480 or higher</p>
Software	<p>The standard browsers for the following operating systems<sup>*1</sup></p> <ul style="list-style-type: none"><li>• Apple iOS 5.0</li><li>• Android 2.1 - 2.3</li><li>• Android 3.1</li><li>• Android 4.0</li></ul>

<sup>\*1</sup> Some parts of the layout may be incorrect depending on the mobile device.

#### Note

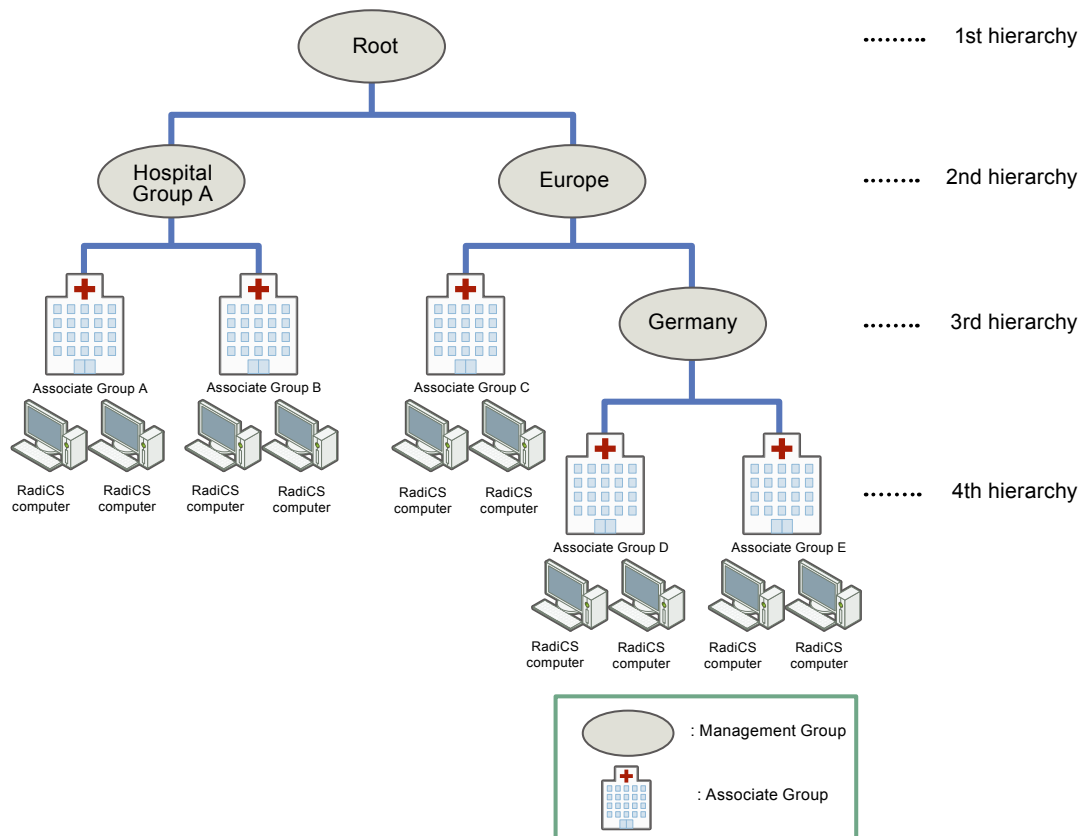
- Refer to “RadiCS User’s Manual” on the RadiCS CD-ROM about System Requirements for RadiCS Computer, compatible sensor, or standards.
- For monitor compatibility, please refer to our website.

# Chapter 2 About Group

## 2-1. Functional Overview of the Group

To manage multiple medical facilities, this system groups the facilities depending on the hierarchy by creating “Group”. This section describes the role of “Group” on this system and the relationship between “Group” and Gateway computer.

### ● What is Group?



- “Group” is a framework with which Gateway computer is managed.
- “Group” has two types, “Associate Group” and “Management Group”.
  - Associate Group: One medical facility
  - Management Group: Use to group Associate Groups
- Group has five-level hierarchy at a maximum. Only one Management Group “Root” exists at the top level.  
\*”Root” cannot be set in RadiNET Pro Web Hosting.

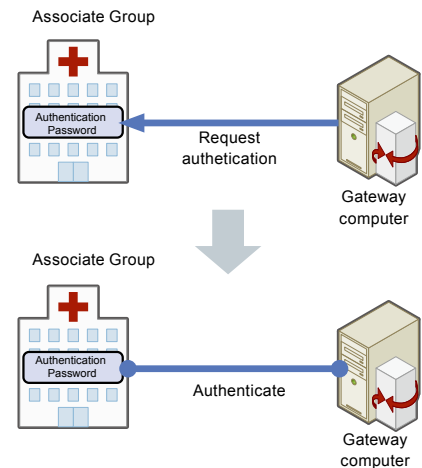


## 2-2. Difference of the RadiNET Pro Gateway Authentication depending on the Group

Authentication password is set to the group. Assigned group is decided with the authentication password specified when RadiNET Pro Gateway is installed. Group is classified into two types, “Associate Group” and “Management Group”, and these types differ in the authentication method as follows.

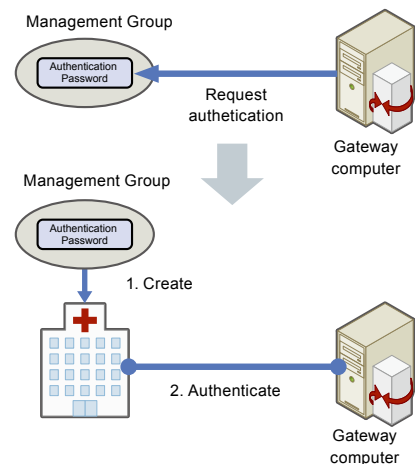
### Using the Authentication Password of Associate Group

When authenticating Gateway computer with the authentication password of “Associate Group”, the associate group and Gateway computer have a one-on-one connection.



### Using the Authentication Password of Management Group

When authenticating Gateway computer with the authentication password of “Management Group”, an associate group is created in the lower level of the authenticated management group, and then the associate group connects to Gateway computer.



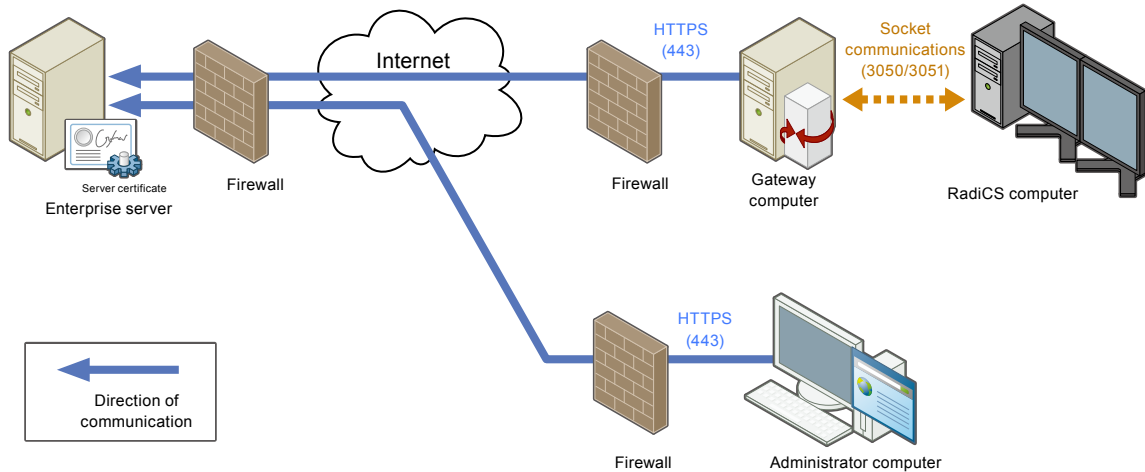
#### Attention

- This system identifies the monitor with the following; Gateway computer that the monitor belongs to, manufacturer, model, and serial number. When the monitor is moved from the Gateway computer that the monitor currently belongs to (called previous Gateway computer) to the other Gateway computer (called new Gateway computer), the monitor that belongs to the new Gateway computer is considered the different monitor from the one that had belonged to the previous Gateway computer. Therefore, the monitor management history on the previous Gateway computer is not taken over. To take over the management history, refer to [“8-2. How to Change Gateway Computers”](#) (page 118).

# Chapter 3 About Network Configuration

## 3-1. Network Configuration of the System

The following communication is used in this system.



### ● HTTPS Communications

HTTPS communications is used in the communications between Enterprise server and Gateway computer, and between Enterprise server and administrator computer. HTTPS encrypts the data with SSL using the server certificate to communicate. Port 443 (TCP) is used in this communication. When installing Gateway computer, only the communication of the port 443 (TCP) for Internet is permitted.

#### Note

Types of Certificate

1. Certificate published by the public certification authority  
Certificate published by the public certification authority, an independent organization. The root certificate of the public certification authority has been registered in advance.
2. Certificate published by the private certification authority  
You can publish an original certificate by establishing a certification authority on Windows Server 2003 / 2008. In that case, a CA certificate needs to be imported to Enterprise server, Gateway computer and administrator computer.

### ● Socket Communications

Socket communications is used in the communication between RadiCS computer and Gateway computer. In this communication, both of RadiCS computer and Gateway computer have two standby ports: 3050 (TCP) and 3051 (TCP). 3050 (TCP) is used for RadiCS and RadiNET Pro Gateway. 3051 (TCP) is used for RadiCS Network Upgrade Software. When installing RadiCS computer and Gateway computer to one computer, the standby ports need to be fixed to eliminate overlap with the other one.

## 3-2. Overview of the System Communication

The communications occur in the following cases.

### 1. Gateway Computer to Enterprise Server

Gateway computer inquires to Enterprise server periodically (default: every 20 minutes) whether there are any remote control requests or setting changes. You can inquire to Enterprise server from Gateway computer manually.

### 2. RadiCS Computer to Gateway Computer

Communications occur, when RadiCS computer needs to download or upload the setting information or send the history data to Enterprise server.

### 3. Gateway Computer to RadiCS Computer

Communications occur, when there are any control requests or setting changes from Enterprise server during the communication of 1.

## 3-3. About Internet Connection

In this system, Enterprise server and Gateway computer are connected via Internet. When selecting the line, refer to the following.

---

#### Note

The volume of data of the communication between Enterprise server and Gateway computer

- The following are the large data to be sent (a few megabyte to 30MB)

- RadiCS update file

This is an update file required for the network upgrade of RadiCS.

- Images for pattern check

This is an image file for use of original pattern check images.

The data is large, but not generated in the daily operation.

- The following are the small data to be sent (a few kilobyte to a few dozen kilobyte)

- Sending and receiving of data files in the daily operation

These are the files used to send or receive the setting information or monitor test result of RadiCS computer.

The data is small, but generated everyday.

---

# SETUP

# Chapter 4 About Administrator Computer

## 4-1. About Administrator Computer

Administrator computer can access the management console of this system by using Internet Explorer.

## 4-2. How to Use Management Console

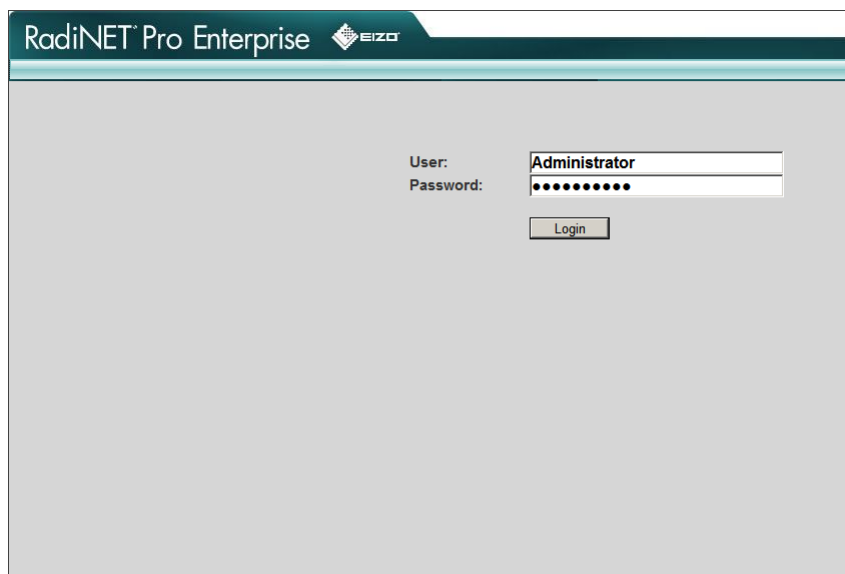
### 1. Run Internet Explorer on the administrator computer.

### 2. Access the relevant URL.

- For RadiNET Pro Enterprise : “https://[domain name]/RadiNETPro/”.
- For RadiNET Pro Web Hosting : URL shown on the registration card

### 3. The login screen appears. Enter the relevant username and password and click [Login].

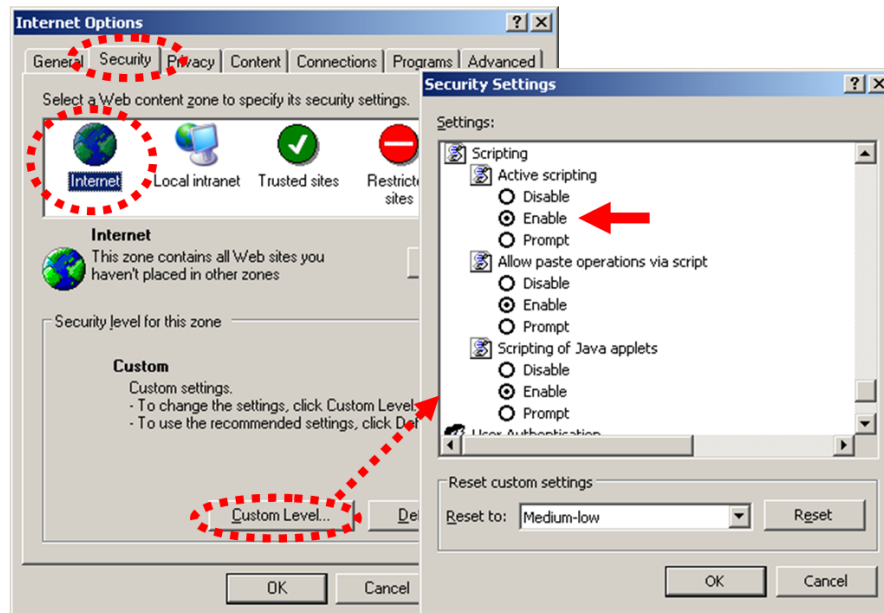
- For RadiNET Pro Enterprise  
User : Administrator  
Password : Password00
- For RadiNET Pro Web Hosting  
Username and password shown on the registration card



The screenshot shows a web browser window with the title "RadiNET Pro Enterprise". The main content area is a login form. It has two input fields: "User:" and "Password:". The "User:" field contains the text "Administrator". The "Password:" field contains a series of dots, representing a masked password. Below the password field is a button labeled "Login".

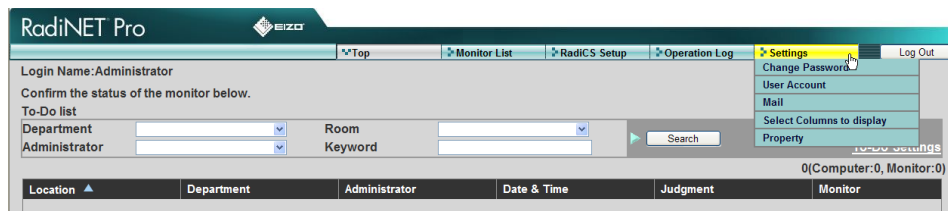
## Settings of Administrator Computer's Browser

- The browser installed on the administrator computer needs to be set as follows.  
[Internet Options] - [Security] - [Internet] - [Custom Level...] - [Active scripting]  
-> Enable

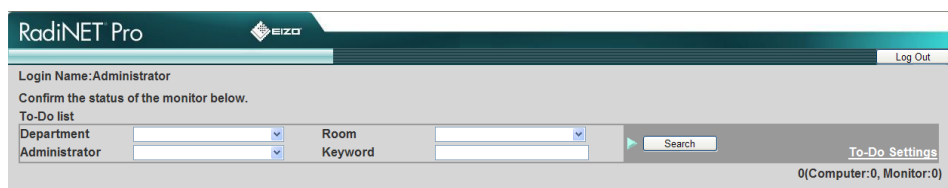


When "Disable" is selected on [Active scripting], the pull-down menu of the "Settings" does not appear on the top page of management console even if you point to it.

- [Internet Options] - [Security] - [Internet] - [Custom Level...] - [Active scripting]  
-> Enable



-> Disable

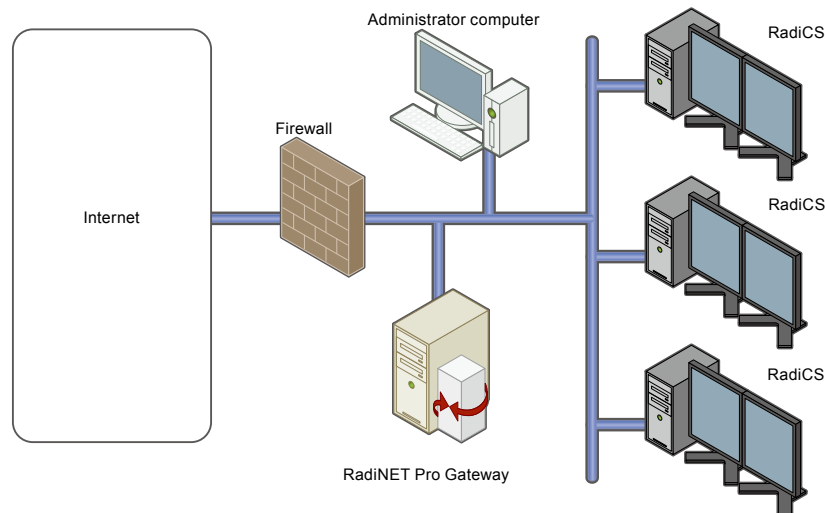


# Chapter 5 Setup of Gateway Computer

## 5-1. About Installation

### When Installing a Large Number of RadiCS Computers in the Hospital

Prepare one computer dedicated for RadiNET Pro Gateway.

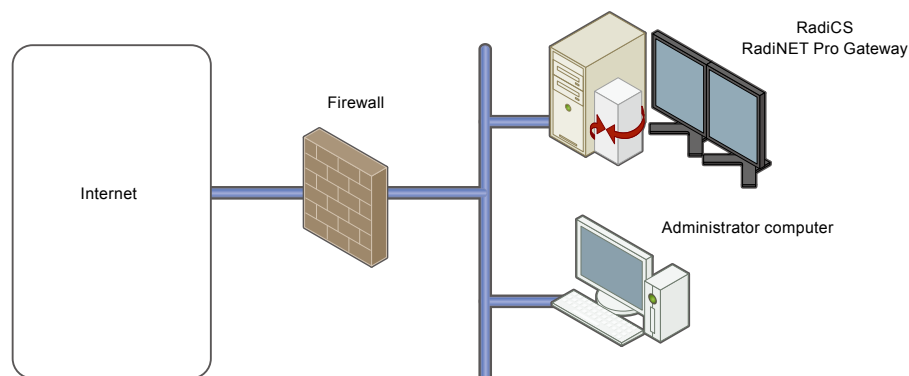


### When Installing Several RadiCS Computers in the Hospital

When the number of RadiCS computers is small (1 to 3), RadiNET Pro Gateway can be installed to each RadiCS computer.

#### Attention

- When installing RadiNET Pro Gateway to RadiCS computer, the port used by RadiNET Pro Gateway and RadiCS overlaps. Therefore, the either port number should be changed. For the details, refer to “5-7. Setting the Port Number for RadiNET Pro Gateway” (page 28), “6-8. Connecting to RadiNET Pro Server” (page 61) and “7-10. Connecting to RadiNET Pro Server” (page 109).
- When the OS of Gateway computer is “Windows XP”, “Windows Vista” or “Windows 7”, please conform the terms of the license before using.
- When the Gateway computer is in sleep mode, RadiNET Pro Gateway may not work correctly. For computers on which RadiNET Pro Gateway is installed, check the sleep setting for Windows, and set the computer so it does not enter the sleep mode.



## 5-2. Preparing Management Group

### Attention

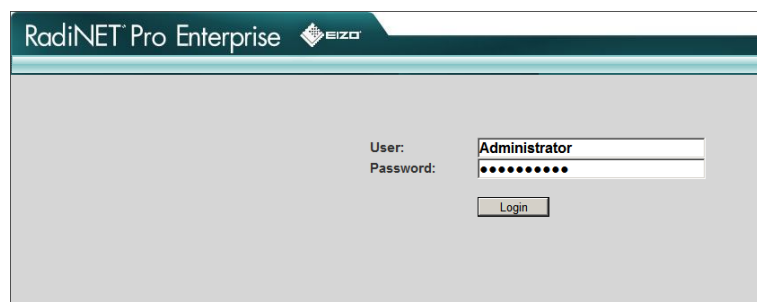
- A management group does not need to be prepared in RadiNET Pro Web Hosting.

Prepare the management group for Gateway computer to connect to Enterprise server. The preparation is performed on the administrator computer.

### Procedure

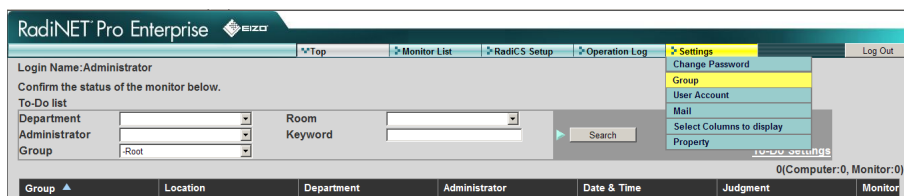
#### 1. From the administrator computer, access the management console.

- URL of management console: `https://[domain name]/RadiNETPro/`
- User at the installation: Administrator
- Password of the user: Password00



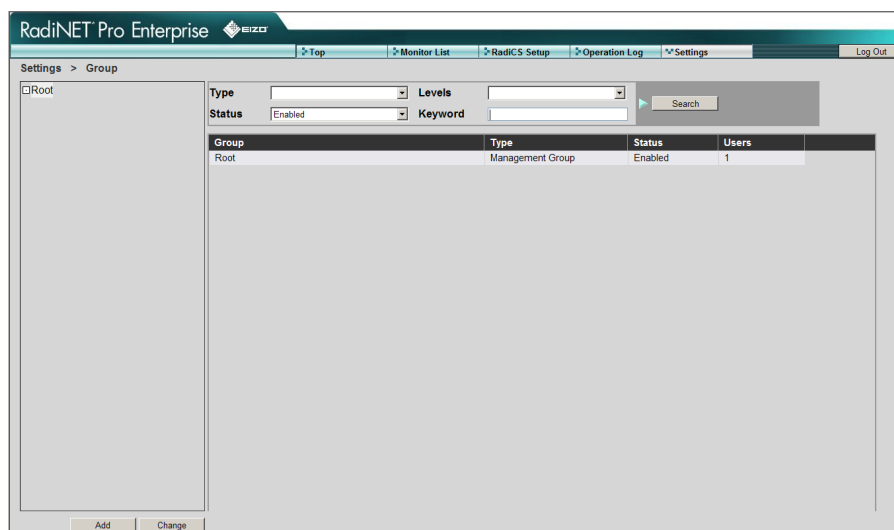
The screenshot shows the login page of the RadiNET Pro Enterprise web application. The header includes the product name and the EIZO logo. The main area contains a login form with fields for 'User:' (containing 'Administrator') and 'Password:' (masked with dots). A 'Login' button is positioned below the password field.

#### 2. Click [Settings] - [Group] from the menu bar of the management console.



The screenshot displays the main management console interface. The top navigation bar includes links for 'Top', 'Monitor List', 'RadiCS Setup', 'Operation Log', 'Settings', and 'Log Out'. The 'Settings' menu is expanded, showing options like 'Change Password', 'Group', 'User Account', 'Mail', 'Select Columns to display', and 'Property'. The 'Group' option is highlighted. Below the navigation bar, there is a section for 'Login Name: Administrator' and a 'To-Do list' with fields for 'Department', 'Room', and 'Group'. A table at the bottom shows a list of groups, with the 'Root' group selected.

#### 3. "Group" screen appears. Click [Change].

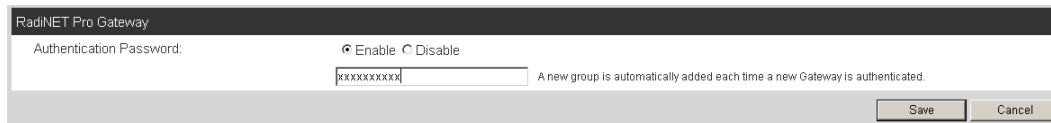


The screenshot shows the 'Group' settings page. The left sidebar contains a tree view with 'Root' selected. The main area displays configuration options for the selected group, including 'Type', 'Status', 'Levels', and 'Keyword'. A 'Search' button is located next to the 'Keyword' field. Below these options is a table showing the details of the 'Root' group.

Group	Type	Status	Users
Root	Management Group	Enabled	1



- 4. The changing screen appears. Select “Enable” of “Authentication Password:”, and then enter password in entry fields. After entering the password, click [Save].**



The screenshot shows a web interface titled "RadlNET Pro Gateway". Below the title, there is a section labeled "Authentication Password:". To the right of this label, there are two radio buttons: "Enable" (which is selected) and "Disable". Below the radio buttons, there is a text input field containing "xxxxxxxxxx". To the right of the input field, there is a small text note: "A new group is automatically added each time a new Gateway is authenticated." At the bottom right of the form, there are two buttons: "Save" and "Cancel".

## 5-3. Installation of .NET Framework

### Note

- For RadiNET Pro Web Hosting, if .NET Framework V4.0 is not installed, follow the steps described in “5-4. Installation of RadiNET Pro Gateway” (page 20) or “5-8. Installation of RadiCS Network Upgrade Software Server” (page 30), and the “Microsoft .NET Framework 4 Setup” screen will automatically be displayed.

### Procedure

#### 1. Display the Setup screen.

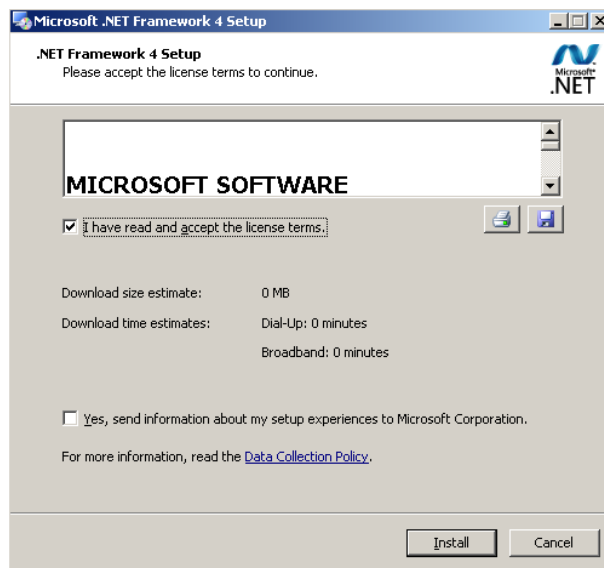
For RadiNET Pro Enterprise : Insert the “RadiNET Pro Enterprise CD-ROM” to the drive.

#### 2. Click “Install .NET Framework V4.0”.

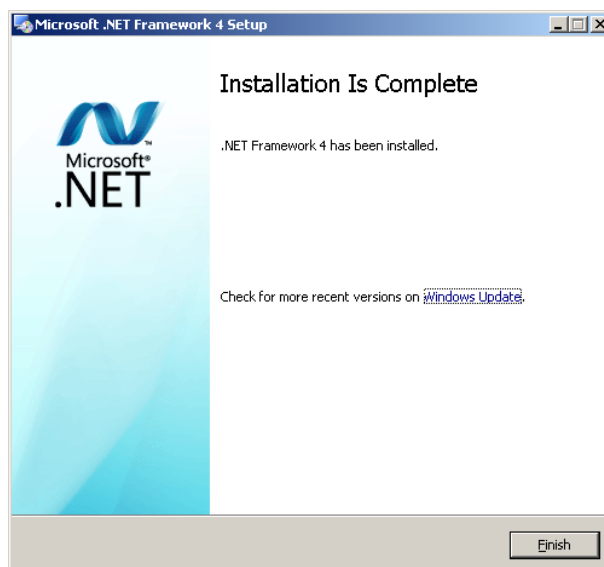


For RadiNET Pro Enterprise

- 3.** The “Microsoft .NET Framework 4 Setup” screen appears. Select “I have read and ACCEPT the terms of the License Agreement” and then click [Install].



- 4.** The “Installation Is Complete” screen appears. Click [Finish].



## 5-4. Installation of RadiNET Pro Gateway

### Procedure

#### 1. Display the Setup screen.

For RadiNET Pro Enterprise : Insert the “RadiNET Pro Enterprise CD-ROM” to the drive.

For RadiNET Pro Web Hosting : Extract the provided ZIP file and execute the setup program.

#### 2. The “EIZO RadiNET Pro Enterprise Setup” screen appears. Click “Install RadiNET Pro Gateway”.

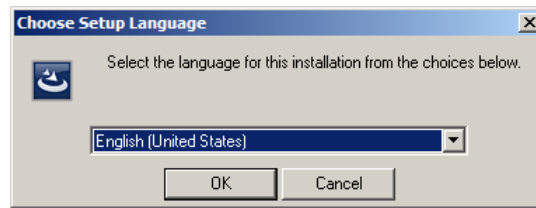


For RadiNET Pro Enterprise

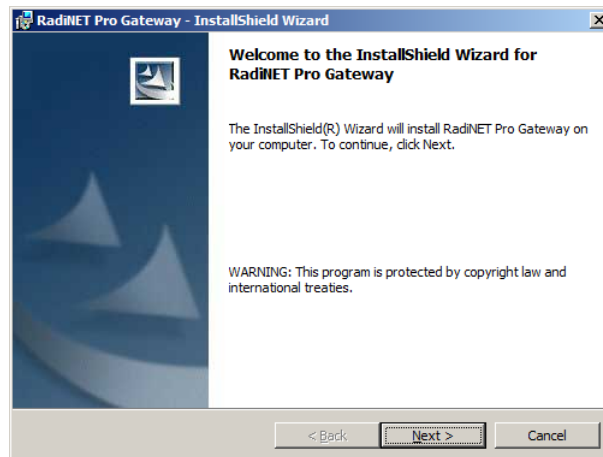


For RadiNET Pro Web Hosting

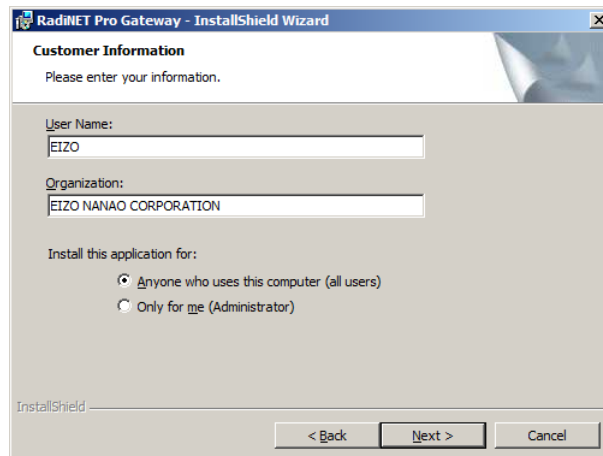
- 3.** The “Choose Setup Language” screen appears. Select the language and click [OK].



- 4.** The “RadiNET Pro Gateway- InstallShield Wizard” screen appears. Click [Next].



- 5. The “Customer Information” screen appears. Check the contents of “User Name:” and “ Organization:”, and then click [Next].**



The screenshot shows the 'Customer Information' screen of the 'RadiNET Pro Gateway - InstallShield Wizard'. The window title is 'RadiNET Pro Gateway - InstallShield Wizard'. The main heading is 'Customer Information' with the instruction 'Please enter your information.' Below this, there are two text input fields: 'User Name:' containing 'EIZO' and 'Organization:' containing 'EIZO NANAO CORPORATION'. Under the heading 'Install this application for:', there are two radio button options: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for me (Administrator)'. At the bottom left is the 'InstallShield' logo. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

- 6. The “Set Password” screen appears. Set password and then click [Next].**

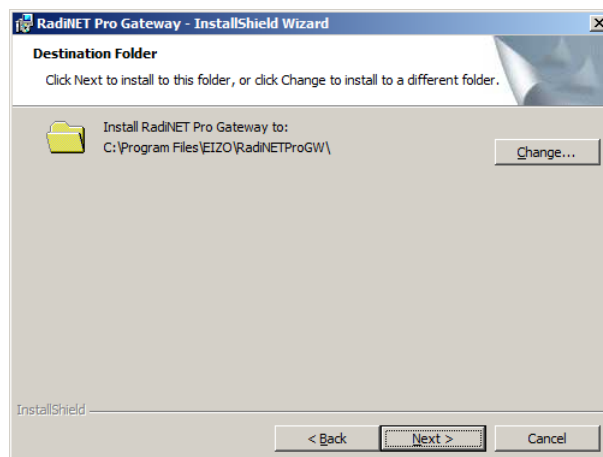
Default password is “GwPassword”.



The screenshot shows the 'Set Password' screen of the 'RadiNET Pro Gateway - InstallShield Wizard'. The window title is 'RadiNET Pro Gateway - InstallShield Wizard'. The main heading is 'Set Password' with the instruction 'Change RadiNET Pro Gateway password.' Below this, there are two password input fields: 'New Password:' and 'Type New Password:', both containing masked characters (dots). At the bottom left is the 'InstallShield' logo. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

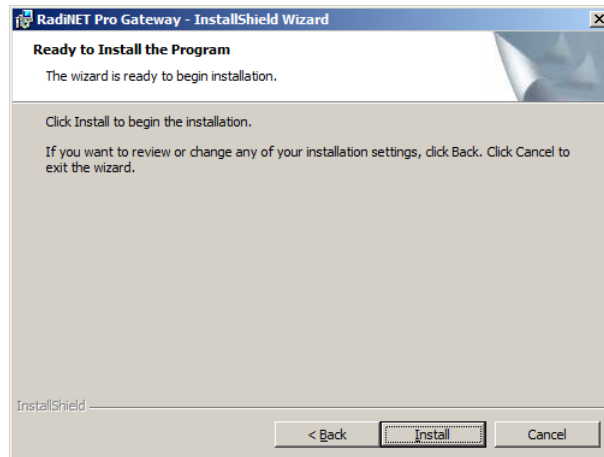
- 7. The “Destination Folder” screen appears. Click [Change...] if you change destination folder. After entering the information, click [Next].**

If you click [Change...], the “Change Current Destination Folder” screen appears. Specify the installation folder and then click [OK].

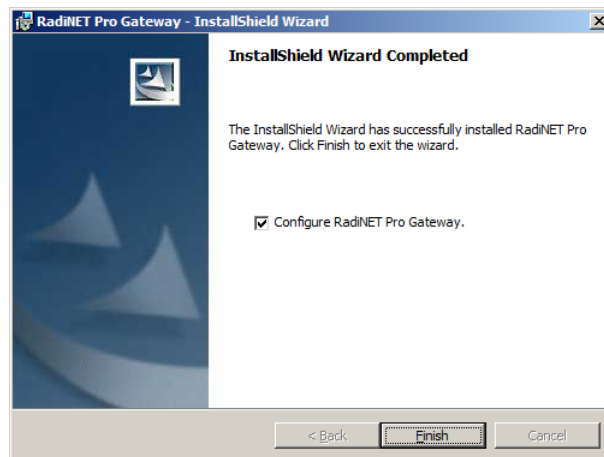


The screenshot shows the 'Destination Folder' screen of the 'RadiNET Pro Gateway - InstallShield Wizard'. The window title is 'RadiNET Pro Gateway - InstallShield Wizard'. The main heading is 'Destination Folder' with the instruction 'Click Next to install to this folder, or click Change to install to a different folder.' Below this, there is a folder icon and the text 'Install RadiNET Pro Gateway to: C:\Program Files\EIZO\RadiNETProGW\'. To the right of this text is a 'Change...' button. At the bottom left is the 'InstallShield' logo. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

**8. The “Ready to Install the Program” screen appears. Click [Install].**



**9. The “InstallShield Wizard Completed” screen appears. Click [Finish].**



**Attention**

- When check “Configure RadiNET Pro Gateway.” checkbox and click [Finish], “RadiNET Pro Gateway” starts.
- “RadiNET Pro Gateway “ can be started by clicking [Start] - [All Programs] - [EIZO] - [RadiNET Pro Gateway] in Windows.

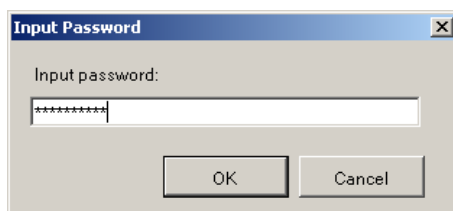
## 5-5. Connecting to Enterprise Server

This section describes how to connect to Enterprise server by using “RadiNET Pro Enterprise Connection Wizard”. “RadiNET Pro Enterprise Connection Wizard” starts after installing RadiNET Pro Gateway or by clicking [Start] - [All Programs] - [EIZO] - [RadiNET Pro Gateway] in Windows.

### Procedure

1. After installing RadiNET Pro Gateway, continuously execute RadiNET Pro Enterprise Connection Wizard, and “Input Password” screen appears. Enter the password that has been set during installation of RadiNET Pro Gateway.

- Default password: GwPassword



2. The “Authentication” screen appears. Enter the information to “Enterprise Server Address:” and “Authentication Password:”, and then click [Next].

- For RadiNET Pro Enterprise

Enterprise Server Address:

Enter the “domain name of the server certificate” of the server to which RadiNET Pro Enterprise is installed.

Authentication Password:

Enter the password of the group that you want to associate with Gateway computer. Set the group with the management console. For the details, refer to “5-2. Preparing Management Group” (page 16).

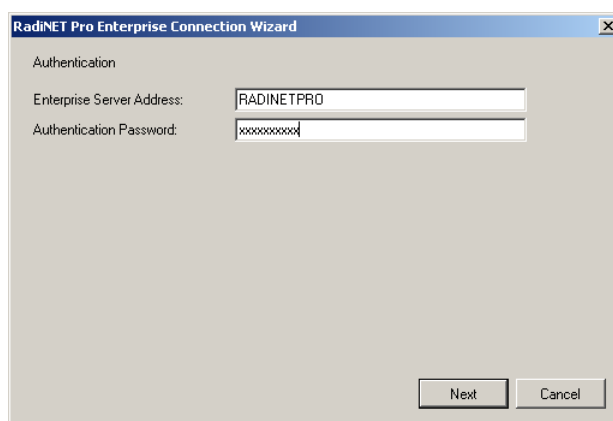
- For RadiNET Pro Web Hosting

Enterprise Server Address:

Enter the Enterprise Server Address shown on the registration card.

Authentication Password:

Enter the Authentication Password shown on the registration card.

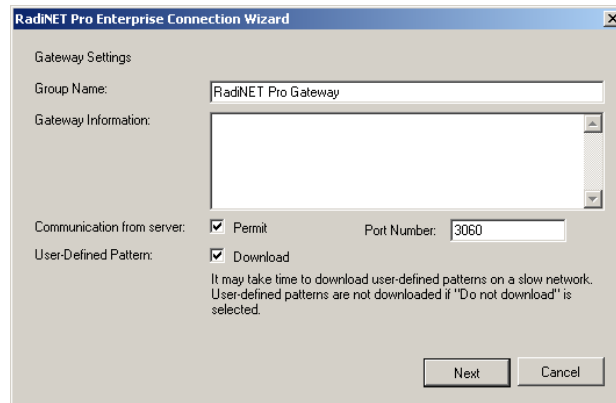




- 3.** The “Gateway Settings” screen appears. Set “Group Name:”, “Gateway Information:” (arbitrary) , “Communication from server” and “User-Defined Pattern:”, and then click [Next].

**Attention**

- “Group Name” is not required for RadiNET Pro Web Hosting.



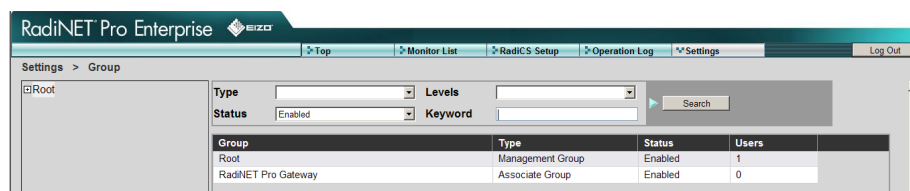
The screenshot shows the 'RadiNET Pro Enterprise Connection Wizard' window. The 'Gateway Settings' tab is active. The 'Group Name' field contains 'RadiNET Pro Gateway'. The 'Gateway Information' field is empty. Under 'Communication from server', the 'Permit' checkbox is checked, and the 'Port Number' is set to '3060'. Under 'User-Defined Pattern', the 'Download' checkbox is checked. A note states: 'It may take time to download user-defined patterns on a slow network. User-defined patterns are not downloaded if "Do not download" is selected.' The 'Next' and 'Cancel' buttons are at the bottom right.

- 4.** The “The Gateway computer has connected to the Enterprise server.” Screen appears. Click [Finish].



The screenshot shows the 'RadiNET Pro Enterprise Connection Wizard' window. The message 'The Gateway computer has connected to the Enterprise server.' is displayed. The 'Finish' button is at the bottom right.

- 5.** On the management console, you can check that Gateway computer is added.



The screenshot shows the 'RadiNET Pro Enterprise' management console. The 'Settings > Group' path is selected. The 'Group' list shows the 'RadiNET Pro Gateway' group. The 'Type' is 'Associate Group', 'Status' is 'Enabled', and 'Users' is '0'.

Group	Type	Status	Users
Root	Management Group	Enabled	1
RadiNET Pro Gateway	Associate Group	Enabled	0

## 5-6. Changing the Query Interval

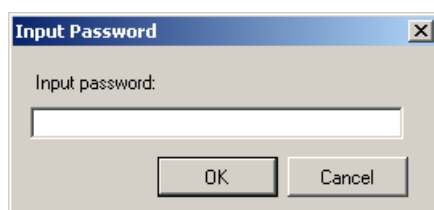
You can change how often Gateway computer queries whether the remote operations to be executed exists on the Enterprise server. This section describes how to change the query interval.

### Attention

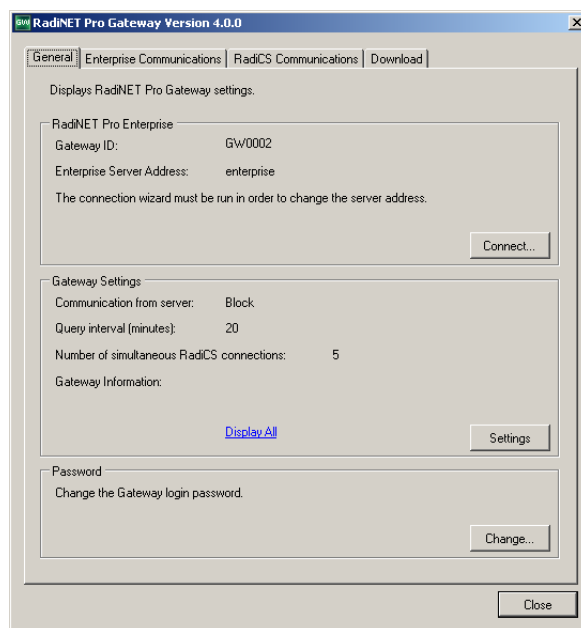
- Shortening the query interval reduces the time required to reflect the remote operations on Enterprise computer in RadiCS computer.
- The minimum value of query interval is “1”, and the maximum is “1440”.

### Procedure

1. Click [Start] - [All Programs] - [EIZO] - [RadiNET Pro Gateway] in Windows.
2. The “Input Password” screen appears. Enter the password and then click [OK].

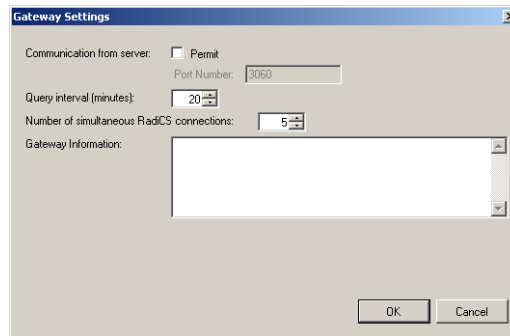


3. The “RadiNET Pro Gateway” screen appears. Select “General” tab, and then click [Settings] in “Gateway Settings”.



**4. The “Gateway Settings” screen appears. Set “Query interval (minutes):” and click [OK].**

- For RadiNET Pro Enterprise : Any numeric value (minutes)
- For RadiNET Pro Web Hosting : 1 minute

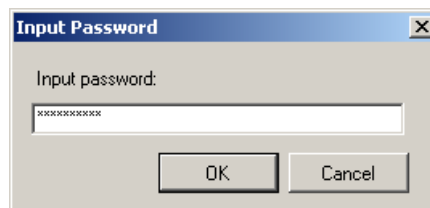


## 5-7. Setting the Port Number for RadiNET Pro Gateway

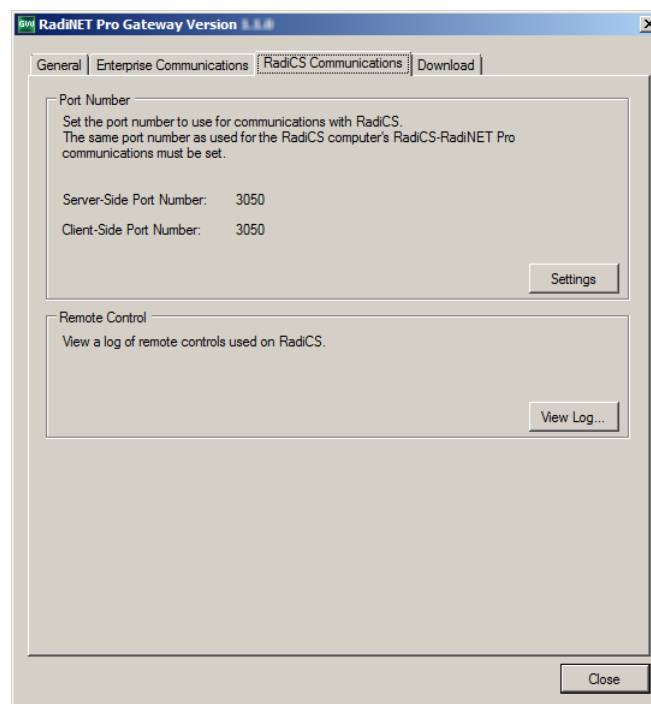
When installing RadiNET Pro Gateway and RadiCS to the same computer, “Server-Side Port Number” and “Client-Side Port Number” need to be changed to different port numbers. When the port numbers have been changed on RadiNET Pro Gateway, the port numbers also need to be changed on RadiCS. About how to change the port numbers on RadiCS, refer to [“6-8. Connecting to RadiNET Pro Server” \(page 61\)](#) and [“7-10. Connecting to RadiNET Pro Server” \(page 109\)](#).

### Procedure

1. Click [Start] - [All Programs] - [EIZO] - [RadiNET Pro Gateway] in Windows.
2. The “Input Password” screen appears. Enter the password and then click [OK].

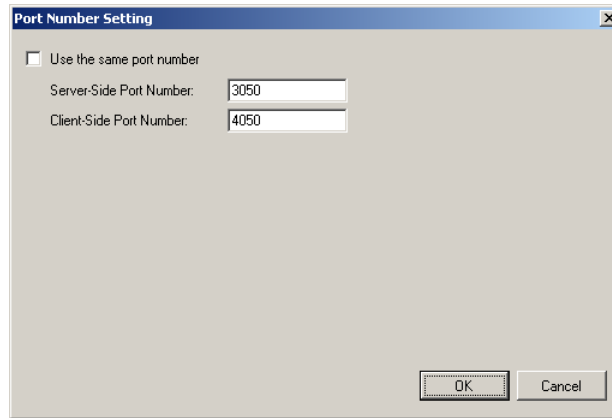


3. Click [Settings] of “RadiCS Communications” tab.



#### 4. The “Port Number Setting” screen appears. Set each item. Click [OK].

- Use the same port number:  
When installing RadiNET Pro Gateway and RadiCS to the same computer, uncheck it.
- Server-Side Port Number:  
Standby port for RadiNET Pro Gateway (Set the port number different from the Client-Side Port Number.)
- Client-Side Port Number:  
Standby port for RadiCS (Set the port number different from the Server-Side Port Number.)



---

**Attention**

- After changing the port number of RadiNET Pro Gateway, the same port number needs to be set as an exception using the Windows firewall setting. Refer to [“5-10. Configuring Windows Firewall” \(page 34\)](#) for details
-

## 5-8. Installation of RadiCS Network Upgrade Software Server

---

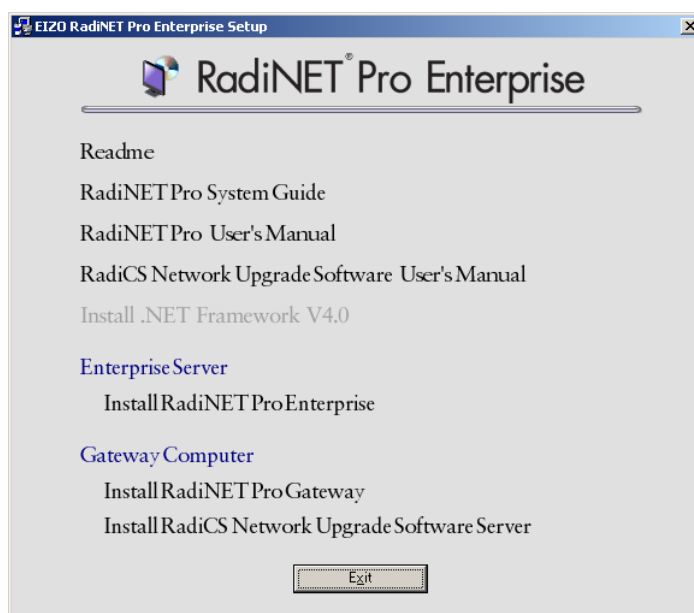
### Procedure

#### 1. Display the Setup screen.

For RadiNET Pro Enterprise : Insert the “RadiNET Pro Enterprise CD-ROM” to the drive.

For RadiNET Pro Web Hosting : Extract the provided ZIP file and execute the setup program.

#### 2. Click “Install RadiCS Network Upgrade Software Server”.

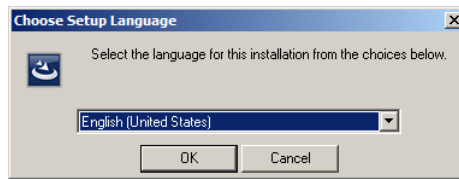


For RadiNET Pro Enterprise

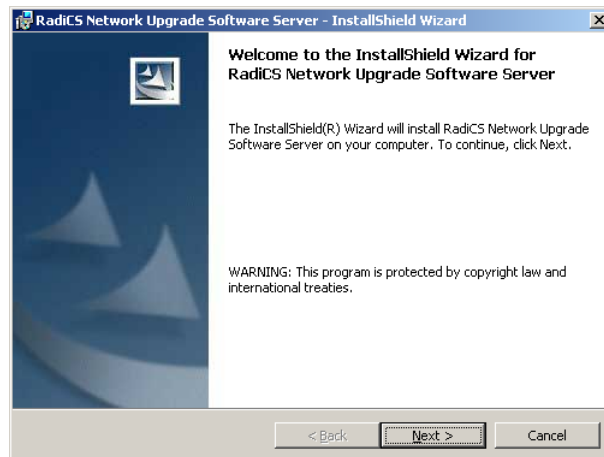


For RadiNET Pro Web Hosting

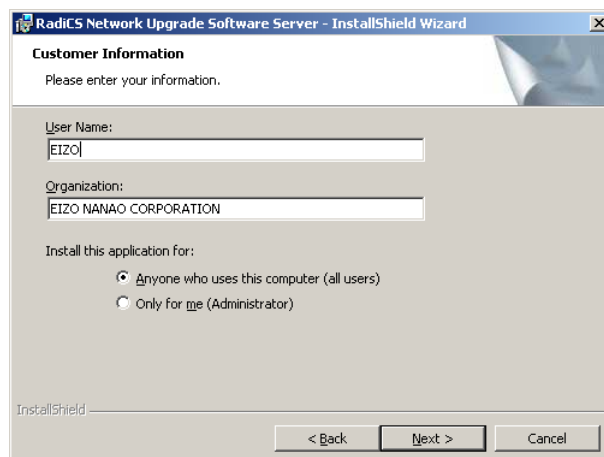
3. The “Choose Setup Language” screen appears. Select the language and click [OK].



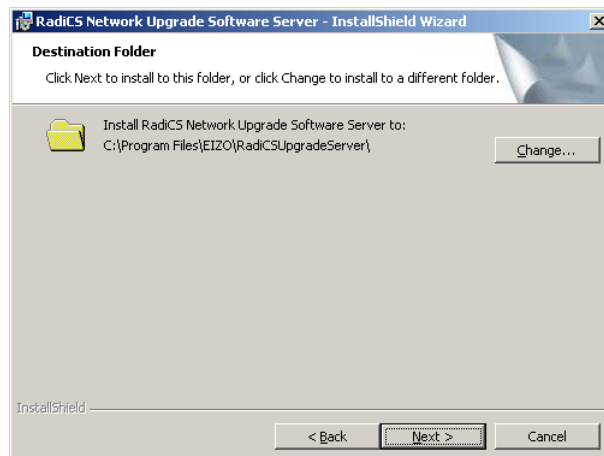
4. The “RadiCS Network Upgrade Software Server - InstallShield Wizard” screen appears. Click [Next].



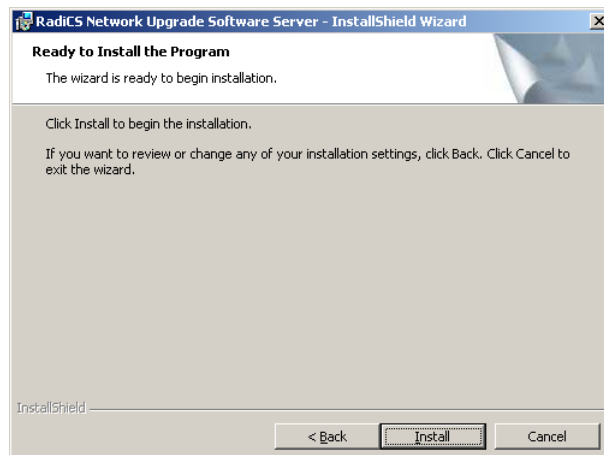
5. The “Customer Information” screen appears. Enter “User Name:” and “Organization:”, and then select “Anyone who uses this computer (all users)”. Click [Next].



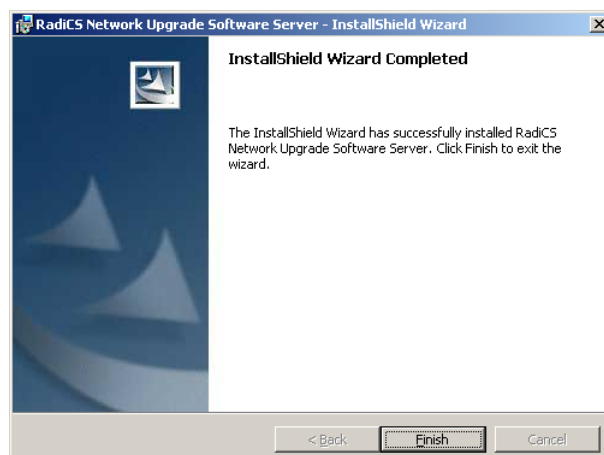
- 6.** The “Destination Folder” screen appears. Click [Change...], and then “Change Current Destination Folder” screen appears. Specify the installation folder and then click [Next].



- 7.** The “Ready to Install the Program” screen appears. Click [Install].



- 8.** The “InstallShield Wizard Completed” screen appears. Click [Finish].



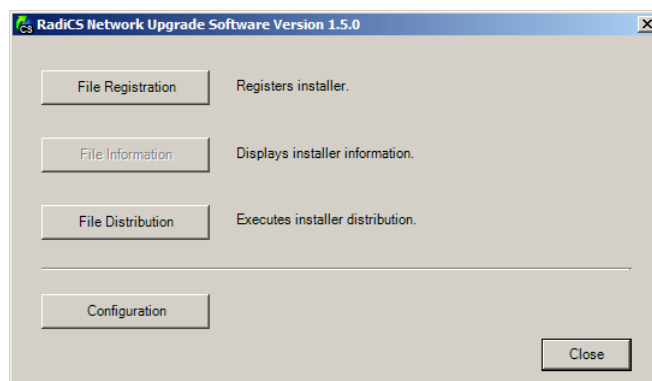


## 5-9. Setting the Port Number for RadiCS Network Upgrade Software

When installing RadiNET Pro Gateway and RadiCS to the same computer, “Server-Side Port Number” and “Client-Side Port Number” need to be changed to different port numbers.

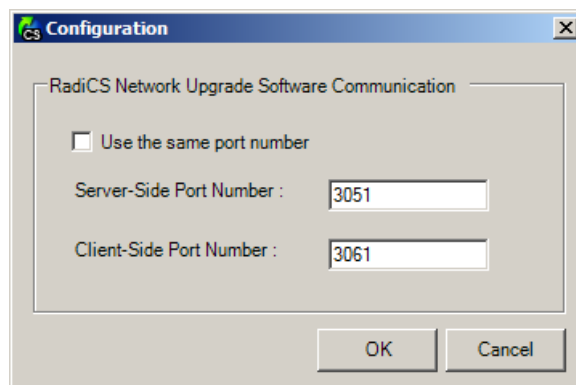
### Procedure

1. Click [Start] - [All Programs] - [EIZO] - [RadiCS Network Upgrade Software] in Windows.
2. Click [Configuration].



3. The “Configuration” screen appears. Set each item. Click [OK].

- Use the same port number:  
Check this to use the same port number for the RadiNET Pro Gateway and RadiCS.  
When installing RadiNET Pro Gateway and RadiCS to the same computer, uncheck it.
- Server-Side Port Number: Standby port for RadiNET Pro Gateway
- Client-Side Port Number: Standby port for RadiCS



## 5-10. Configuring Windows Firewall

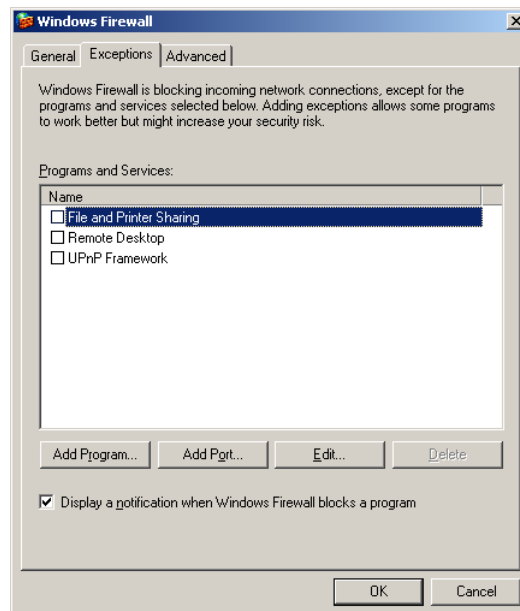
When “Windows Firewall” is enabled on Gateway computer, Windows firewall is configured automatically during the installation of RadiNET Pro Gateway. If you need to setup the “Windows Firewall” manually, perform the “Enable Program Communications”.

### Enable Port Communications

#### ● For Windows XP / Vista / Server 2003

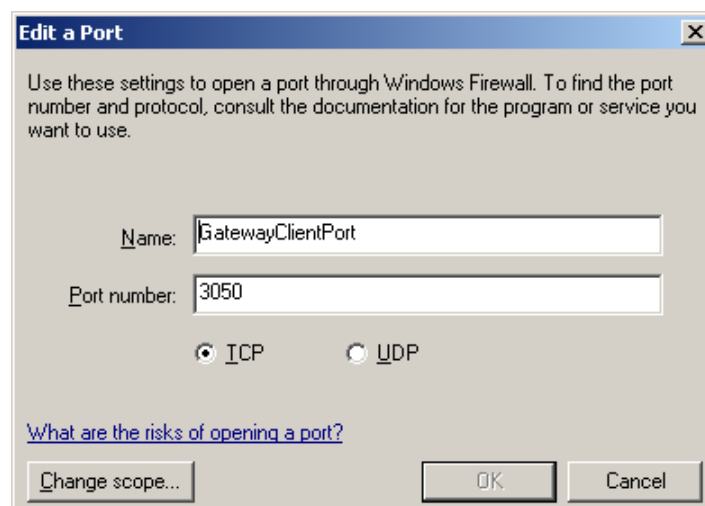
#### Procedure

1. Select [Windows Firewall] from [Control Panel] in Windows.
2. The “Windows Firewall” screen appears. Select the “Exceptions” tab and then click [Add Port].



3. The “Edit a Port” screen appears. Set the following and then click [OK].

- Name: GatewayClientPort
- Port number: 3050



**4.** Click [Add Program] again.

**5.** The “Edit a Port” screen appears. Set the following and then click [OK].

- Name: GatewayServerPort
- Port number: 3060

**Edit a Port**

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: GatewayServerPort

Port number: 3060

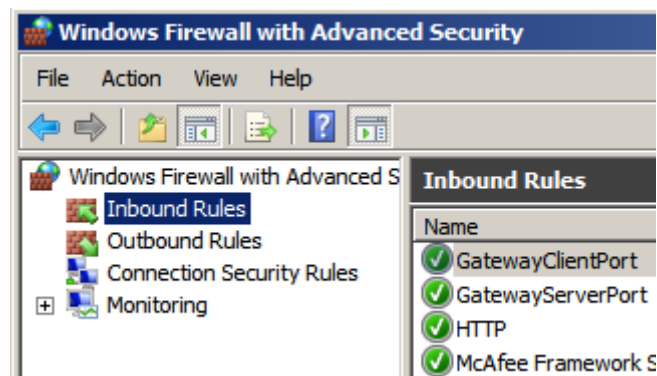
☒ TCP ☐ UDP

[What are the risks of opening a port?](#)

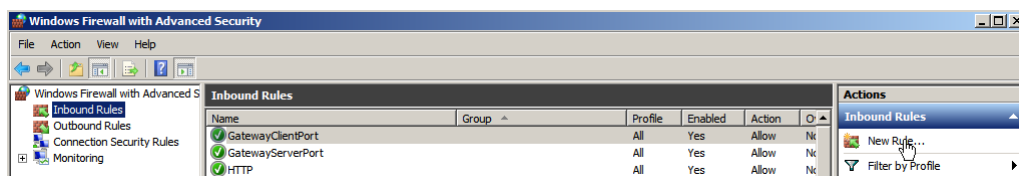
Change scope... OK Cancel

## ● Windows 7 / Server 2008 / 2008 R2

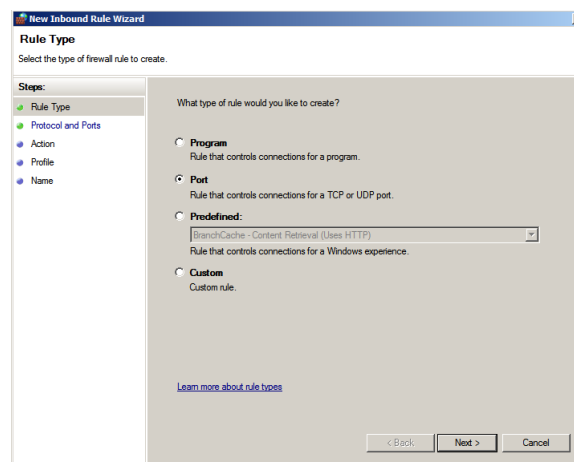
1. Click [System and Security] - [Windows Firewall] from [Control Panel] and then click [Advanced]. From the left side of the screen, click “New Rule”.



2. From the right side of the screen, click “New Rule”.



3. “Rule Type” screen appears. Select “Port” and click [Next].



4. “Protocol and Ports” screen appears. Input “3050” to “Specific local ports”. Then click [Next].

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar shows the progression: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area asks 'Does this rule apply to TCP or UDP?' with 'TCP' selected. Below, it asks 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports' selected and the value '3050' entered in the text box. A link 'Learn more about protocol and ports' is at the bottom. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

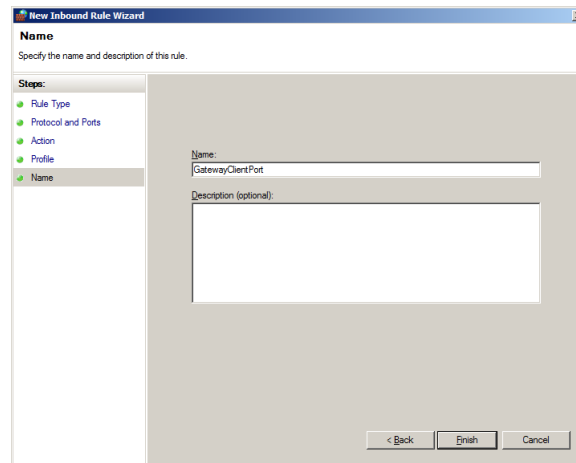
5. “Action” screen appears. Select “Allow the connection” and then click [Next].

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar shows the progression: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?' with three options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. A 'Customize' button is next to the second option. A link 'Learn more about actions' is at the bottom. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

6. “Profile” screen appears. Select all and then click [Next].

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The left sidebar shows the progression: Rule Type, Protocol and Ports, Action, Profile (selected), and Name. The main area asks 'When does this rule apply?' with three checked options: 'Domain' (Applies when a computer is connected to its corporate domain), 'Private' (Applies when a computer is connected to a private network location), and 'Public' (Applies when a computer is connected to a public network location). A link 'Learn more about profiles' is at the bottom. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

- 7. “Name” screen appears. Input “GatewayClientPort” to “Name” and click [Finish].**



- 8. Perform the same steps to set the following.**

- Name: GatewayServerPort
- Port number: 3060

.....



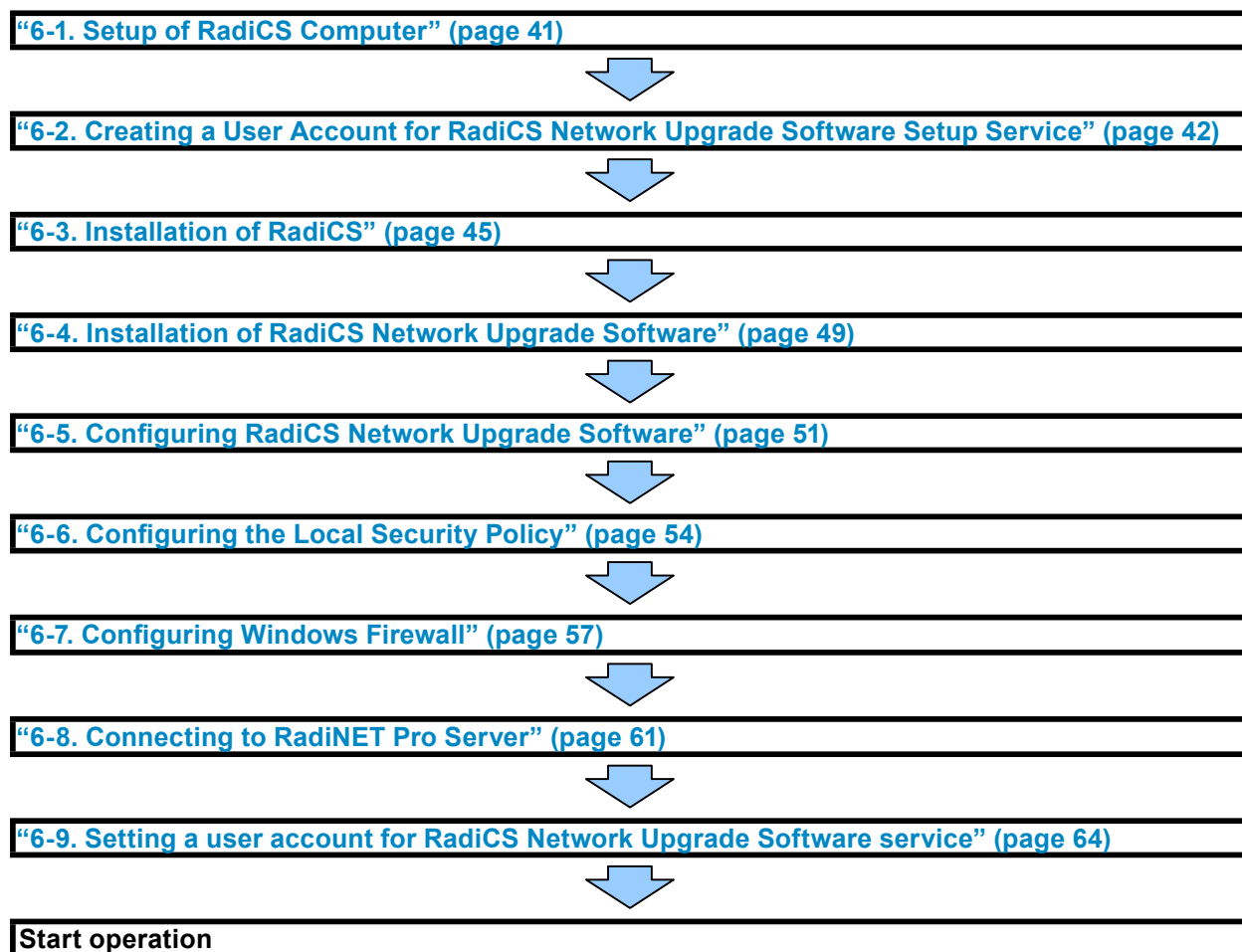
# Chapter 6 Setup of RadiCS Computer (WORKGROUP)

There are two types of networks formed by Windows: workgroup-based networks and domain-based networks. Care must be taken that the setup procedure for the RadiCS computer varies depending on which network you are in. When using the RadiCS computer in the domain-based environment, refer to “Chapter 7 Setup of RadiCS Computer (DOMAIN)” (page 67).

## WORKGROUP

Each computer manages its users and resources (files, folders, printers, etc.) individually. Every computer performs its own user/resource management, hence the user management is required for each computer used. Therefore, the workgroup option is suitable for creating a small-scale network.

The setup flow of RadiCS computer (WORKGROUP) is the following.



\* If the Windows firewall function is active during the installation of RadiCS, the communication with a required program will be enabled. If you need to configure Windows Firewall manually, refer to “6-1. Setup of RadiCS Computer” (page 41).



## 6-1. Setup of RadiCS Computer

---

### Procedure

- 1. Prepare a suitable computer for RadiCS system requirements.**
- 2. Install the graphics card in the computer according to the installation manual supplied with the graphics card.**
- 3. Connect the EIZO Monitor and the computer with the signal cable and USB cable.**
- 4. Install the device driver of graphics card according to the installation manual supplied with the graphics card.**

## 6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service

This section describes how to create a new user for the RadiCS Network Upgrade Software service.

### Attention

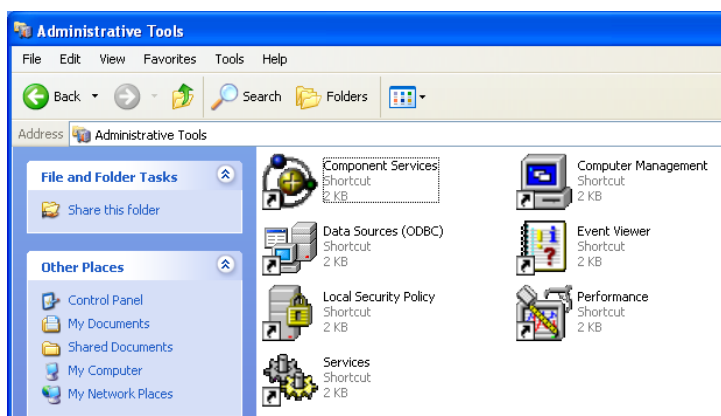
- The user account with administrator authority is required for RadiCS Network Upgrade Software user.
- The built-in administrator user account can be used.
- The user account with administrator authority is required to operate the following procedure.

### Procedure

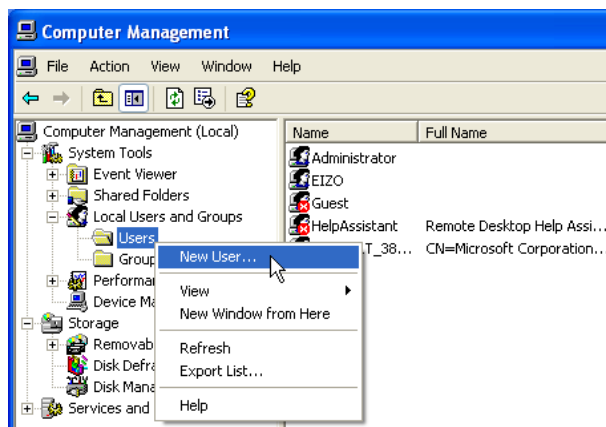
#### 1. Click [Performance and Maintenance] - [Administrative Tools] - [Computer Management] from [Control Panel] in Windows.

### Note

- For Windows Vista, click [System and Maintenance] - [Administrative Tools] - [Computer Management] from [Control Panel] in Windows.
- For Windows 7, click [System and Security] - [Administrative Tools] - [Computer Management] from [Control Panel] in Windows.

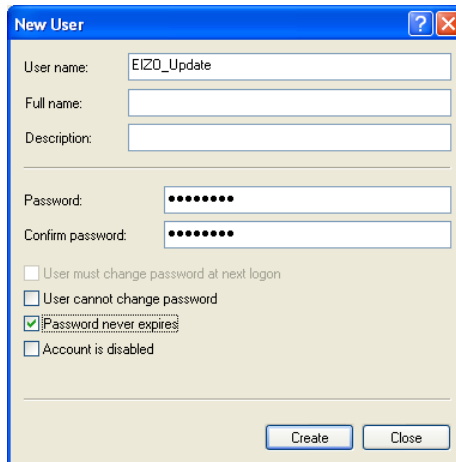


#### 2. The “Computer Management” screen appears. From the left side of the screen, select “Local Users and Groups”. Select “Users”. Click the right mouse button and then select [New User...] from the menu.

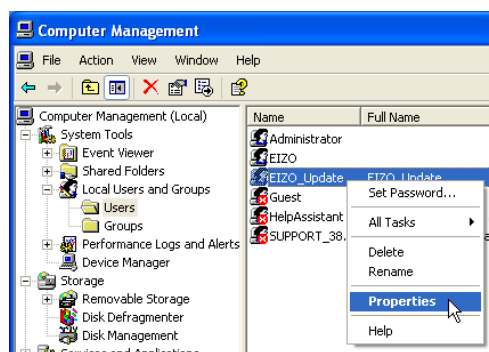


**3. The “New User” screen appears. Set the followings and click [Create].**

- User name: Enter start up user of RadiCS Network Upgrade Software Service
- Password and Confirm password: Enter password to logon
- Password never expires: Check

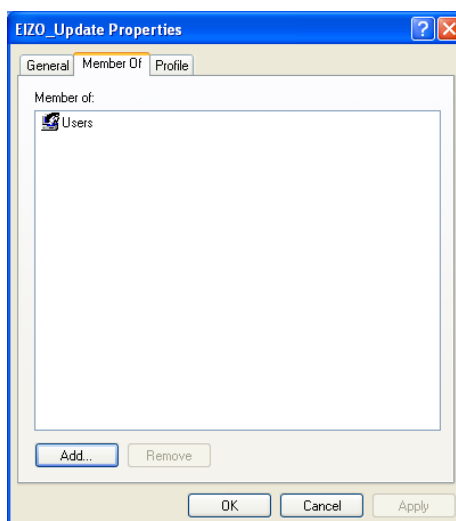


**4. The “Computer Management” screen reappears, select the created account and click the right mouse button. Select [Properties] from the menu.**



**5. “[User Accounts] Properties” screen appears. Select “Member Of” tab.**

**6. “Member Of” tab appears. Click [Add...].**



**7. The “Select Group” screen appears. Click [Advanced].**

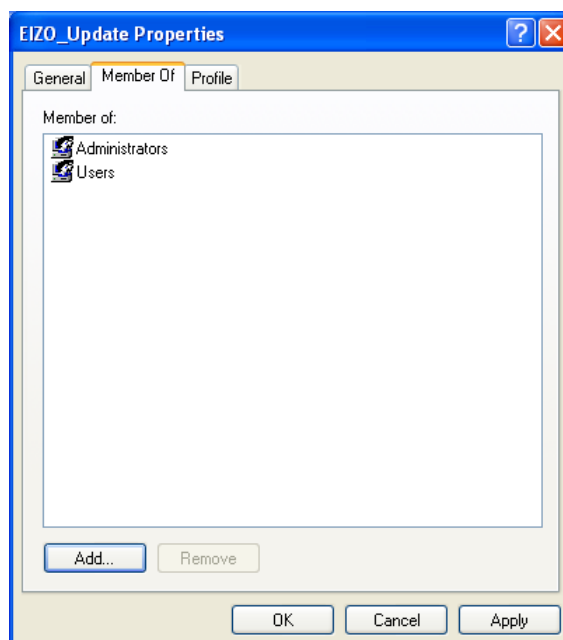
**8.** The detailed setting screen appears. Click [Find Now].

**9.** Select [Administrators] from the list. Click [OK].

Name (RDN)	In Folder
Administrators	EIZO-PC
Backup Oper...	EIZO-PC
Guests	EIZO-PC
HelpServices...	EIZO-PC
Network Confi...	EIZO-PC
Power Users	EIZO-PC
Remote Desk...	EIZO-PC
Replicator	EIZO-PC
Users	EIZO-PC

**10.** The “Select Group” screen reappears. Click [OK].

**11.** The “[User name] Properties” screen reappears. Click [OK].



## 6-3. Installation of RadiCS

---

The user account with administrator authority is required to install RadiCS.

---

**Note**

- “Windows Installer Ver.3.1” is installed automatically.
- 

### Procedure

- 1.** Insert the “RadiCS CD-ROM” to the drive and install RadiCS.
- 2.** The “EIZO RadiCS Setup” screen appears. Click “Install RadiCS”.

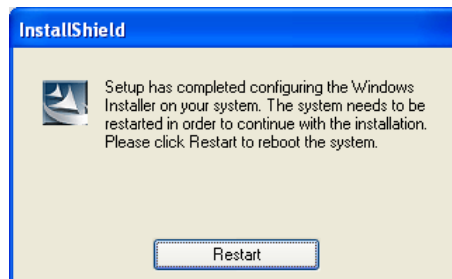


- 3.** You are prompted to restart the computer. Click [Restart].

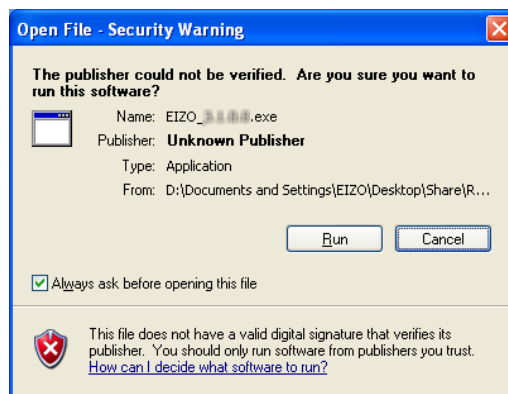
---

**Note**

- No prompt to restart the computer appears on Windows Vista or Windows 7.



- 4.** After restarting Windows, “Open File - Security Warning” screen may appear. Click [Run].



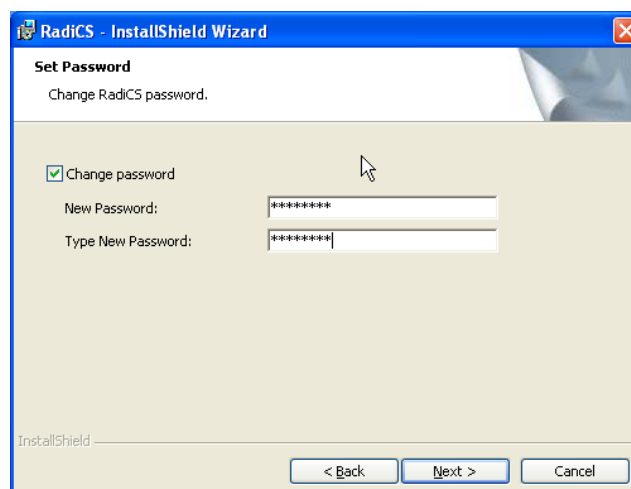
- 5.** The “RadiCS - InstallShield Wizard” screen appears. Click [Next].



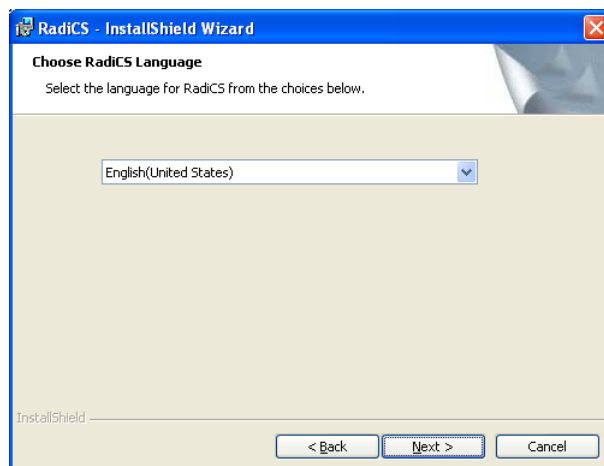
- 6.** The “License Agreement” screen appears. Select “I accept the terms in the license agreement” and then click [Next].

- 7.** The “Set Password” screen appears. Set password and then click [Next].

Default password is “password”.

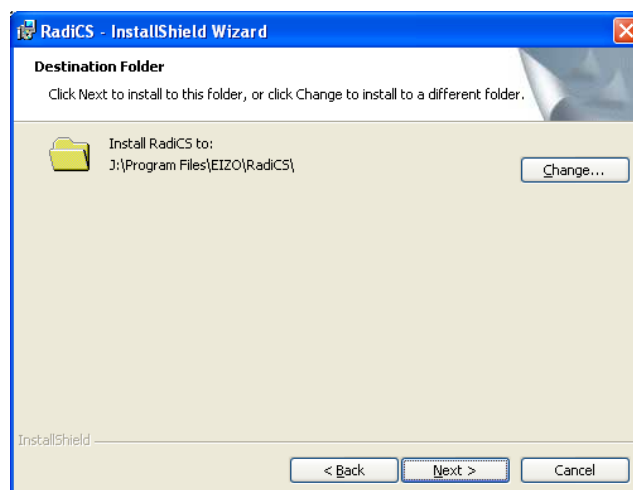


- 8.** The “Choose RadiCS Language” screen appears. Select the language and then click [Next].



- 9.** The “Destination Folder” screen appears. Click [Change...] if you change destination folder. Click [Next].

If you click [Change...], the “Change Current Destination Folder” screen appears. Specify the installation folder and then click [OK].

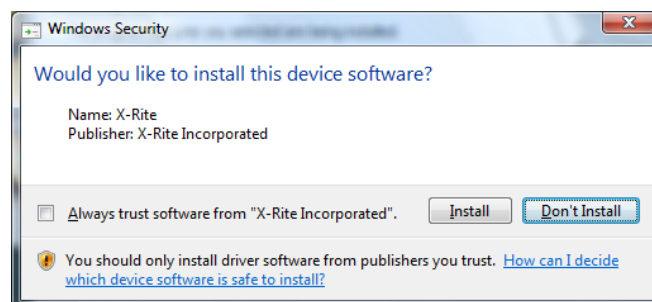


- 10.** The “Ready to Install the Program” screen appears. Click [Install].

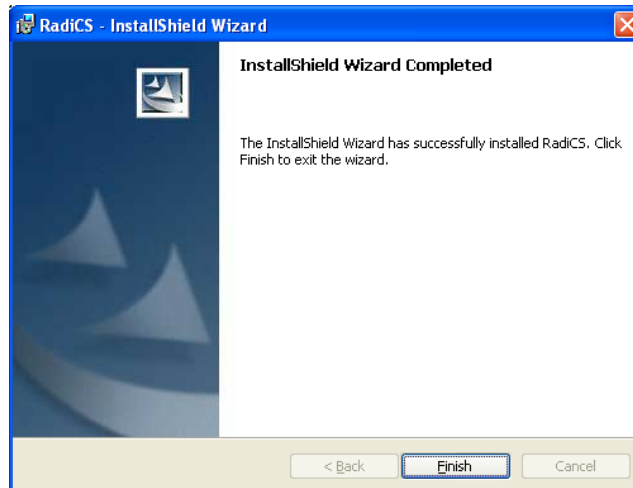
---

**Note**

- For Windows Vista or Windows 7, “Windows Security” screen appears during installation, and you are asked whether to install the device software of “X-Rite”. In that case, click [Install].



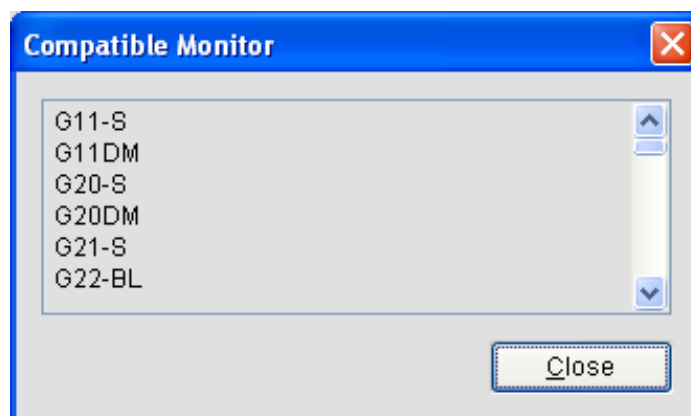
## 11. The “InstallShield Wizard Completed” screen appears. Click [Finish].



---

### Note

- Click the “Compatible Monitor” in the “EIZO RadiCS Setup” screen to see “Compatible Monitor”.  
If the model name of your monitor is not shown there, execute “RadiCS\_MonitorFile\_x.x.x.exe” on the EIZO LCD Utility Disk (CD-ROM) supplied with your monitor.





## 6-4. Installation of RadiCS Network Upgrade Software

### Note

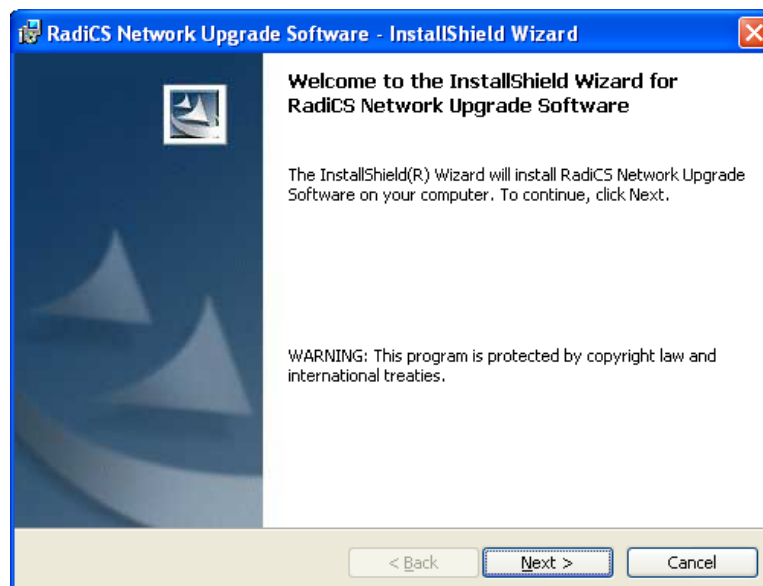
- “.NET Framework 2.0” is installed automatically.

### Procedure

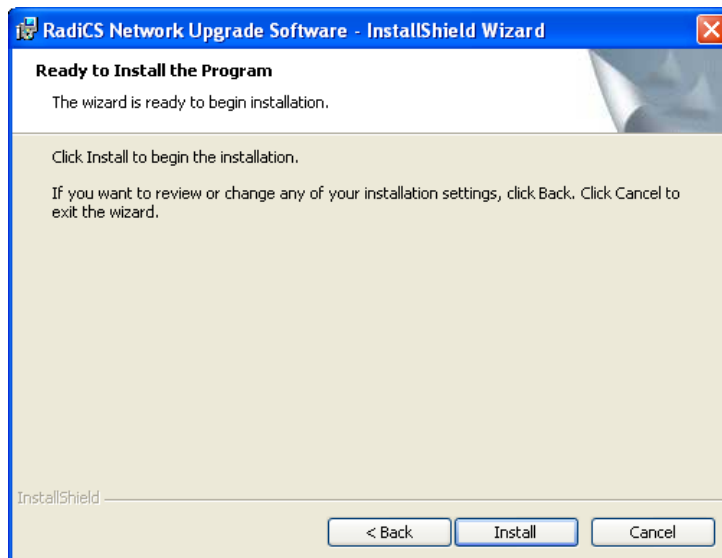
1. Insert the “RadiCS CD-ROM” to the drive.
2. The “EIZO RadiCS Setup” screen appears. Click “Install RadiCS Network Upgrade Software”.



3. The “RadiCS Network Upgrade Software - InstallShield Wizard” screen appears. Click [Next].



**4. The “Ready to Install the Program” screen appears. Click [Install].**



**5. The “InstallShield Wizard Completed” screen appears. Click [Finish].**



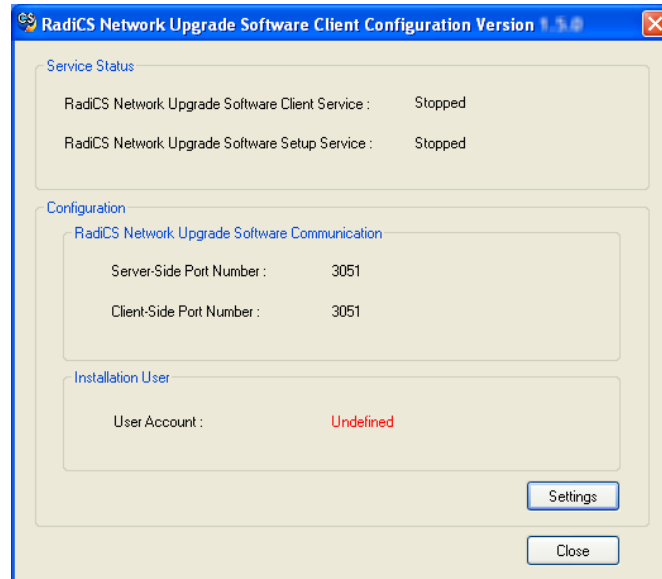
**Attention**

- When “Configure RadiCS Network Upgrade Software” is selected and [Finish] is clicked, “RadiCS Network Upgrade Software Client Configuration” starts.
- “RadiCS Network Upgrade Software Client Configuration” can be started from [Start] - [All Programs] - [EIZO] - [RadiCS Network Upgrade Software Client Configuration] in Windows.

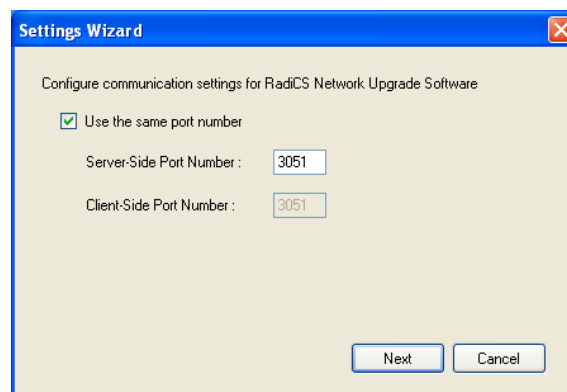
## 6-5. Configuring RadiCS Network Upgrade Software

### Procedure

1. Either continue from “6-4. Installation of RadiCS Network Upgrade Software” (page 49) to perform the settings, or click [Start] - [All Programs] - [EIZO] - [RadiCS Network Upgrade Software Client Configuration] in Windows.
2. The “RadiCS Network Upgrade Software Client Configuration” screen appears. Click [Settings].



3. The “Settings Wizard” screen appears. If the change of communication port is required, set the following and click [Next]. If the change of communication port is not required, click [Next].
  - Use the same port number: Select this to use the same port number for the RadiNET Pro server / Gateway computer (RadiCS Network Upgrade Software Server) and RadiCS computer (RadiCS Network Upgrade Software Client). (This is the default setting)
  - Server-Side Port Number: Set the port number for the RadiCS Network Upgrade Software
  - Client-Side Port Number: Set the port number for the RadiCS Network Upgrade Software Client. When [Use the same port number] is selected, the same port number as [Server-Side Port Number] is used



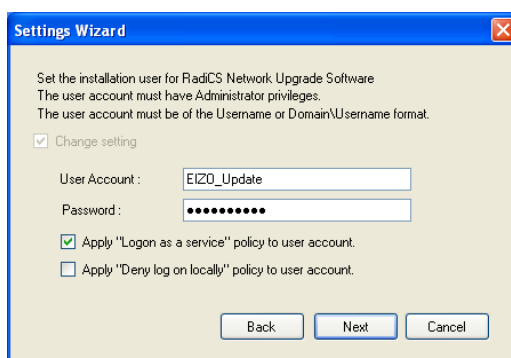
#### 4. The setting screen of user for RadiCS Network Upgrade Software Service appears. Set the following and click [Next].

- User Account: Enter the user name created in “6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 42)
- Password: Enter password of the user entered in User Account
- Apply “Logon as a service” policy to user account: When using user account in Local, select this. When using user account in Domain, unselect this
- Apply “Deny log on locally” policy to user account: Select this only if an exclusive RadiCS network upgrade user was created in “6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 42).

---

**Attention**

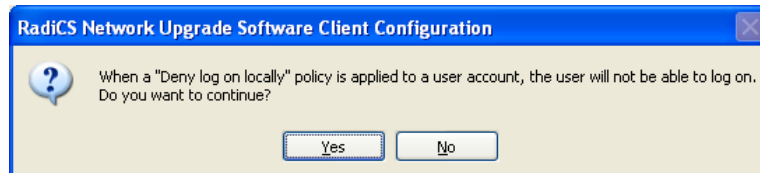
- If “Apply “Deny log on locally” policy to user account” is selected, logging on with that account will no longer be possible.
  - If “Apply “Deny log on locally” policy to user account” is selected for a user account with administrator authority that you are currently using, it may become impossible to log on to Windows.
- 



---

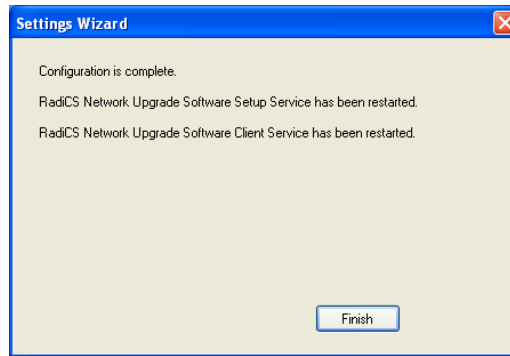
**Note**

- If you select “Apply “Deny log on locally” policy to user account” and then click [Next], the confirmation screen appears. Click [Yes].



- If “Apply “Logon as a service” policy to user account” is selected, the user entered in User Account is added to the local security policy of “Local Policies” - “User Rights Assignment” - “Log on as a service”.
  - If “Apply “Deny log on locally” policy to user account” is selected, the user entered in User Account is added to “Local Policies” - “User Rights Assignment” - “Deny log on locally” of the local security policy.
-

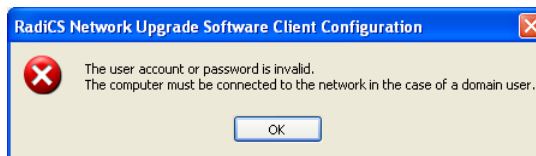
## 5. The “Configuration is complete.” screen appears. Click [Finish].



---

### Note

- The error message is displayed if “User Account” or “Password” is invalid. Enter the correct “User Account” or “Password” again.



- The information about security policy is in [“6-6. Configuring the Local Security Policy”](#) (page 54).
  - When set the user for the RadiCS Network Upgrade Software service manually, refer to [“6-9. Setting a user account for RadiCS Network Upgrade Software service”](#) (page 64).
-

## 6-6. Configuring the Local Security Policy

Assign the “Log on as a service” authority for RadiCS Network Upgrade Software user. RadiCS Network Upgrade Software service cannot be started without the authority.

### Attention

- These settings are made automatically as part of “RadiCS Network Upgrade Software Client Configuration”. If you need to make settings directly, follow the procedure below.

### Procedure

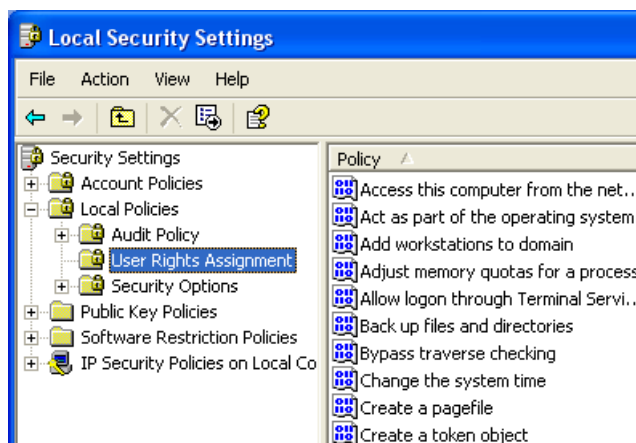
#### 1. Click [Performance and Maintenance] - [Administrative Tools] from [Control Panel] and then double click [Local Security Policy] in Windows.

### Note

- For Windows Vista, click [System and Maintenance] - [Administrative Tools] from [Control Panel] and then double click [Local Security Policy].
- For Windows 7, click [System and Security] - [Administrative Tools] from [Control Panel] and then double click [Local Security Policy].

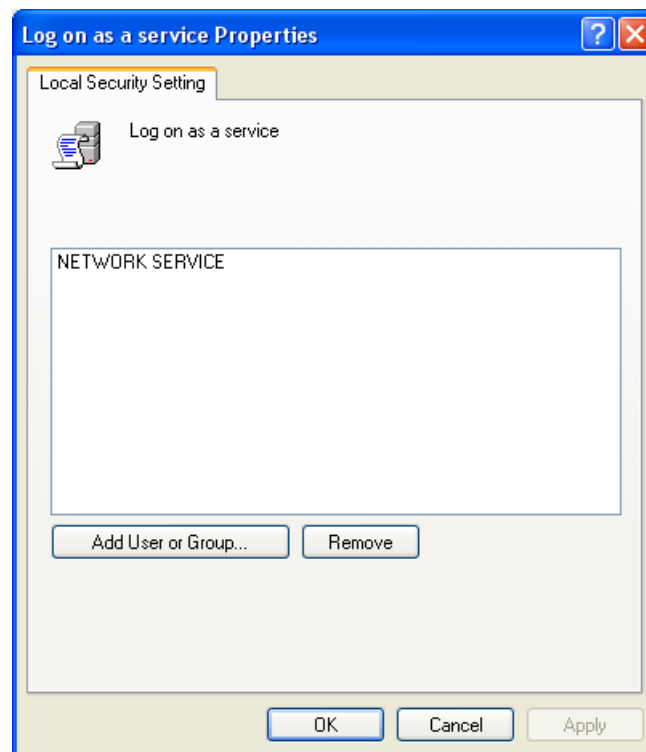


#### 2. The “Local Security Settings” screen appears. From the left side of the screen, select “Local Policies” - “User Rights Assignment”.



#### 3. From the right side of the screen, double click “Log on as a service” and open [Properties].

- 4.** The “Log on as a service Properties” screen appears. Click [Add User or Group...].



- 5.** The “Select Users or Groups” screen appears. Click [Advanced...].
- 6.** The detailed setting screen appears. Click [Find Now].
- 7.** The user account in the computer is listed. Select the user account for RadiCS Network Upgrade Software and the click [OK].

Name (RDN)	In Folder
CREATOR G...	
CREATOR O...	
DIALUP	
EIZO_Update	EIZO-PC
Everyone	
Guest	EIZO-PC
HelpAssistant	EIZO-PC
INTERACTIVE	

## 8. The “Log on as a service Properties” screen reappears. Click [OK].

---

**Note**

- The security of the newly created user account for the RadiCS Network Upgrade Software Service will be improved by selecting “Deny logon locally”, as this will prevent the service user from logging on interactively. The setting procedure is as follows.

1. Click [Performance and Maintenance] - [Administrative Tools] from [Control Panel] and then double click [Local Security Policy] in Windows.

---

**Note**

- For Windows Vista, click [System and Maintenance] - [Administrative Tools] from [Control Panel] and then double click [Local Security Policy].
- For Windows 7, click [System and Security] - [Administrative Tools] from [Control Panel] and then double click [Local Security Policy].

- 
2. The “Local security settings” screen appears. From the right side of the screen, select “Deny logon locally” and then open [Properties].
  3. The “Deny logon locally Properties” screen appears. Click [Add User or Group...].
  4. The “Select Users or Groups” screen appears. Click [Advanced...].
  5. Click [Find Now].
  6. The user account in the computer is listed. Select the user created in [“6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service” \(page 42\)](#) and click [OK].
  7. The “Deny logon locally Properties” screen reappears. Click [OK].
-



## 6-7. Configuring Windows Firewall

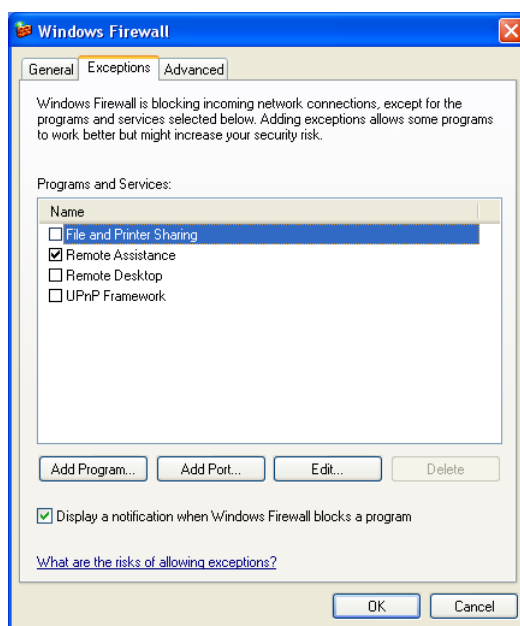
If you need to setup the Windows Firewall manually, perform the “Enable Program Communications” operations.

### Enable Program Communications

#### ● For Windows XP / Vista

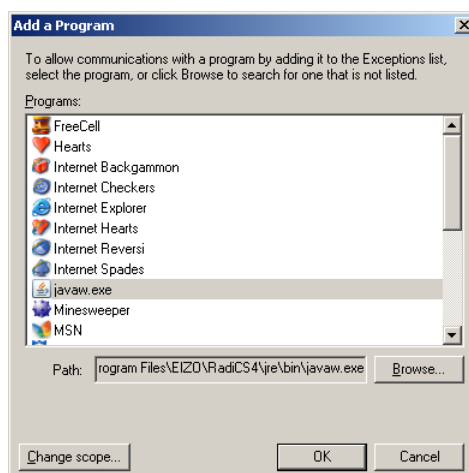
#### Procedure

1. Select [Windows Firewall] from [Control Panel] in Windows.
2. The “Windows Firewall” screen appears. Select the “Exceptions” tab and then click [Add Program...].



3. The “Add a Program” screen appears. Click [Browse...] and set “Path:” by selecting the following program.

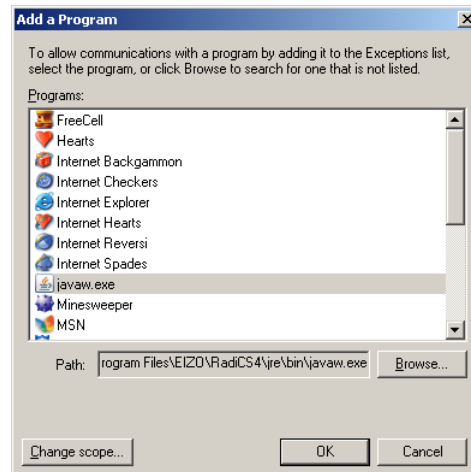
- javaw.exe  
( C:\Program Files\EIZO\RadiCS4\jre\bin\javaw.exe)



**4. Click [Add Program...] again.**

**5. The “Add a Program” screen appears. Click [Browse...] and set “Path:” by selecting the following program.**

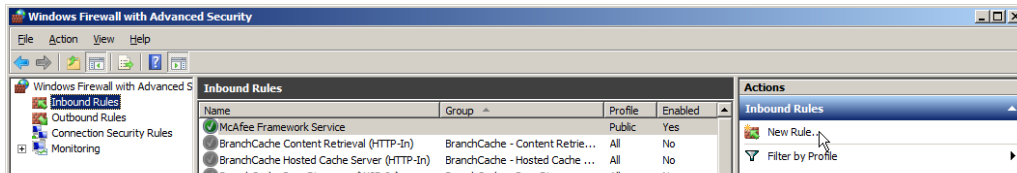
- RadiCSUpdateClientService.exe  
(ex. C:\Program Files\EIZO\RadiCSUpgrade\RadiCSUpdateClientService.exe)



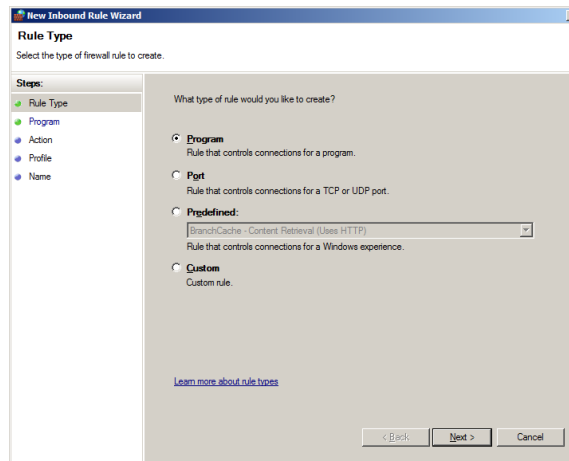
## ● For Windows 7

### Procedure

1. Click [System and Security] - [Windows Firewall] from [Control Panel] and then click [Advanced].
2. The “Windows Firewall with Advanced Security” screen appears. Click “Inbound Rules” and then click “New Rule”.

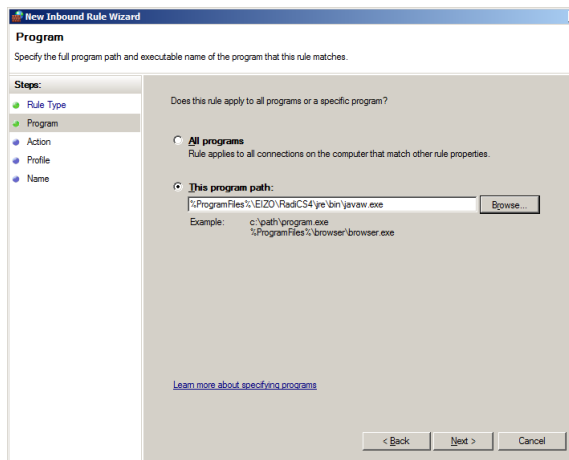


3. “Rule Type” screen appears. Select “Program” and click [Next].

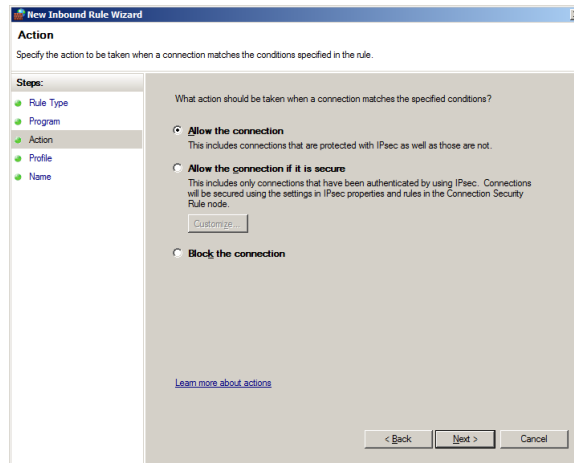


4. “Program” screen appears. Select the following program and click [Next].

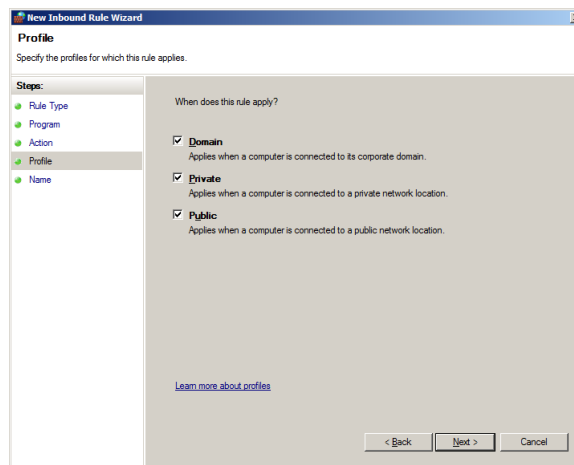
- javaw.exe  
( C:\Program Files\EIZO\RadiCS4\jre\bin\javaw.exe)



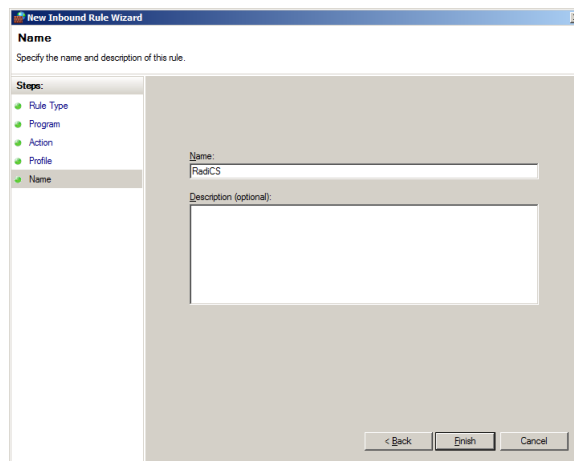
## 5. “Action” screen appears. Click [Next].



## 6. “Profile” screen appears. Click [Next].



## 7. “Name” screen appears. Input name and click [Finish].



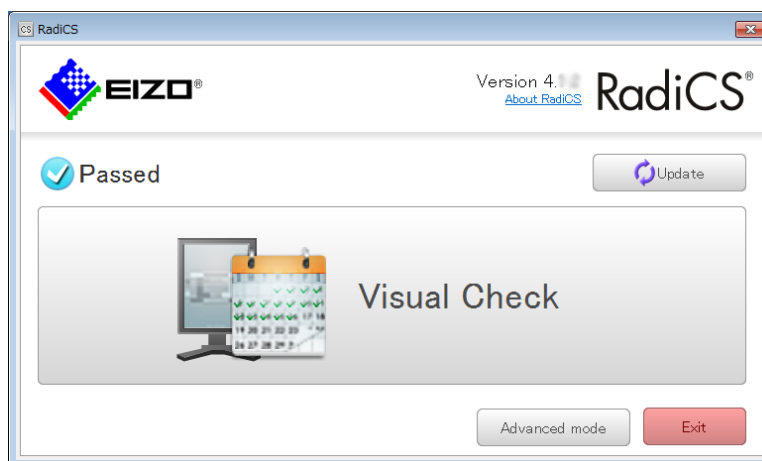
## 6-8. Connecting to RadiNET Pro Server

### Attention

- Although a “connection error” occurs after the following settings in an environment where RadiNET Pro is not running, this does not affect the operation. Once RadiNET Pro starts running, the connection will be established (excluding RadiNET Pro Web Hosting).
- A security system on the network may restrict the communications. In that case, it must be configured so that the communications are enabled.
- For RadiNET Pro :  
Two-way communications must be enabled between the RadiNET Pro server and the RadiCS computer.
- For RadiNET Pro Enterprise / RadiNET Pro Web Hosting :  
Communications must be enabled between the Enterprise Server, Gateway computer, and RadiCS computer.

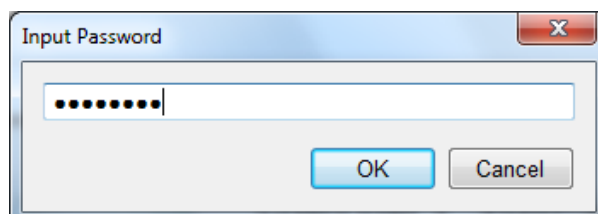
### Procedure

1. Click [Start] - [All Programs] - [EIZO] - [RadiCS] to start RadiCS. Click [Advanced mode]

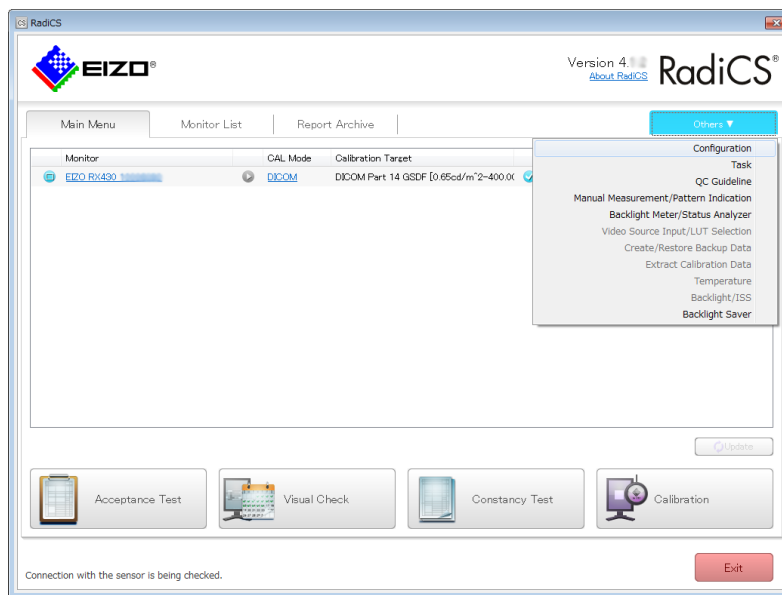


2. The “Input Password” screen appears. Enter the password that was set for installation, and click [OK].

If the password is not changed during RadiCS installation, the password is “password”.



**3. “Advanced mode” starts up. Click [Other] tab and click [Configuration] in the list.**



**4. The “Configuration” screen appears. Click “RadiNET Pro”. Configure the following settings and then click [Apply].**

- Select “Use RadiNET Pro”
- RadiNET Pro Server Address: Enter the address of RadiNET Pro server<sup>\*1</sup>
- Server-Side Port Number: Set the port number for the RadiNET Pro server<sup>\*2</sup>
- Client-Side Port Number: Set the port number for the RadiCS.

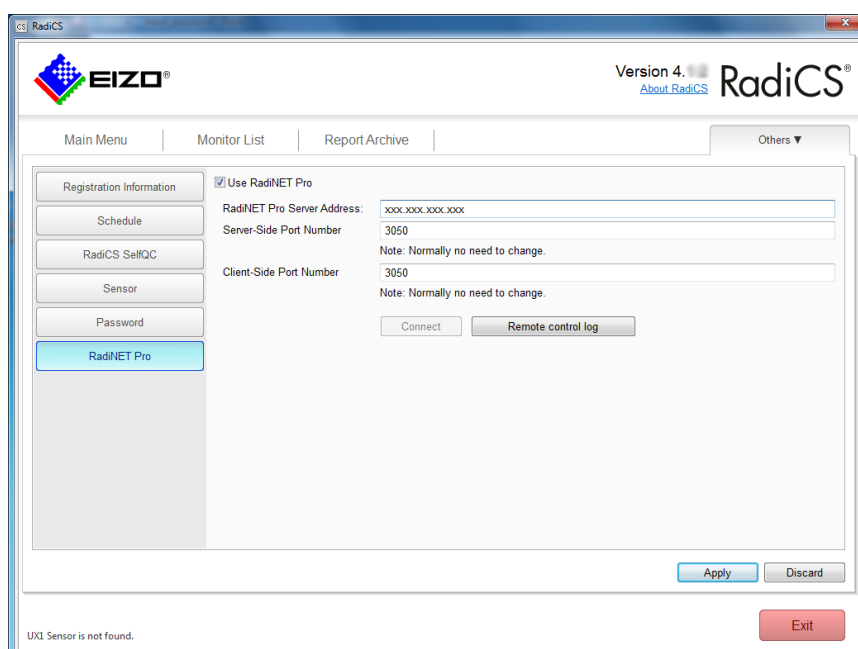
**Attention**

- The port number setting should match the setting of RadiNET Pro.<sup>\*3</sup>

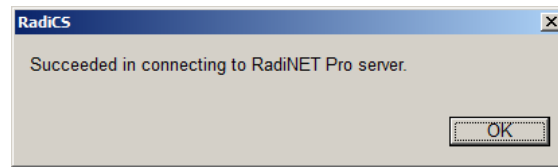
<sup>\*1</sup> For RadiNET Enterprise / RadiNET Pro Web Hosting, enter the address of Gateway computer.

<sup>\*2</sup> For RadiNET Enterprise / RadiNET Pro Web Hosting, set the port number for the Gateway computer.

<sup>\*3</sup> For RadiNET Enterprise / RadiNET Pro Web Hosting, the port number setting should match the setting of Gateway computer.



- 5.** When the connection completed successfully, “Succeeded in connecting to RadiNET Pro server.” message is displayed.



## 6-9. Setting a user account for RadiCS Network Upgrade Software service

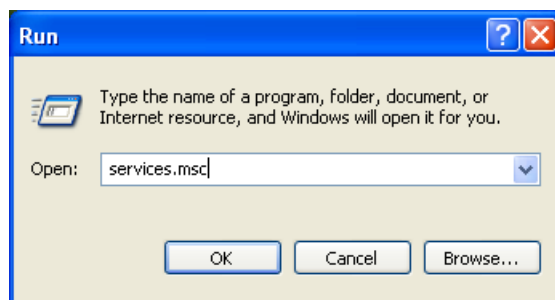
Set the user account for RadiCS Network Upgrade Software Service.

### Attention

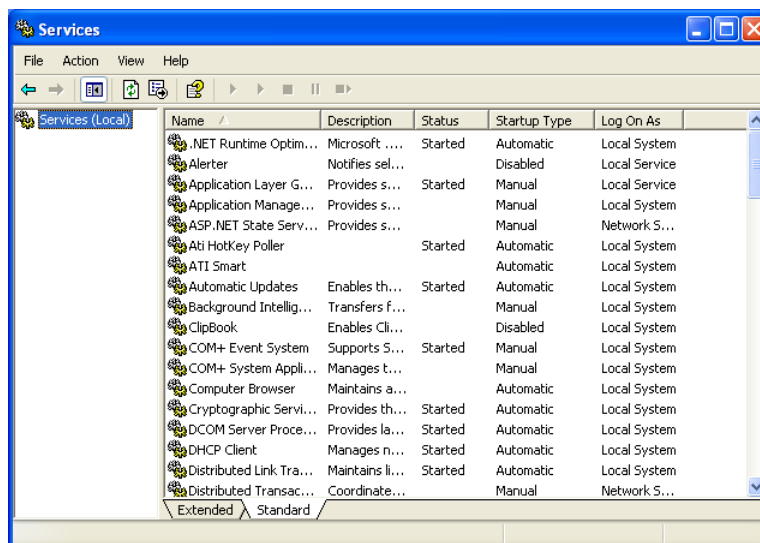
- These settings are made automatically as part of “RadiCS Network Upgrade Software Client Configuration”. If you need to make settings directly, follow the procedure below.

### Procedure

1. Click [Start] - [Run...] in Windows. Enter “services.msc” to “Open:” and then click [OK].

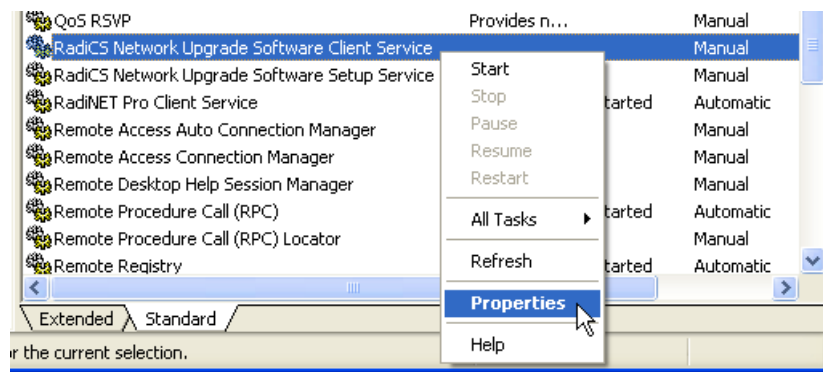


2. The “Services” screen appears. The service list is displayed on the right side of the screen.

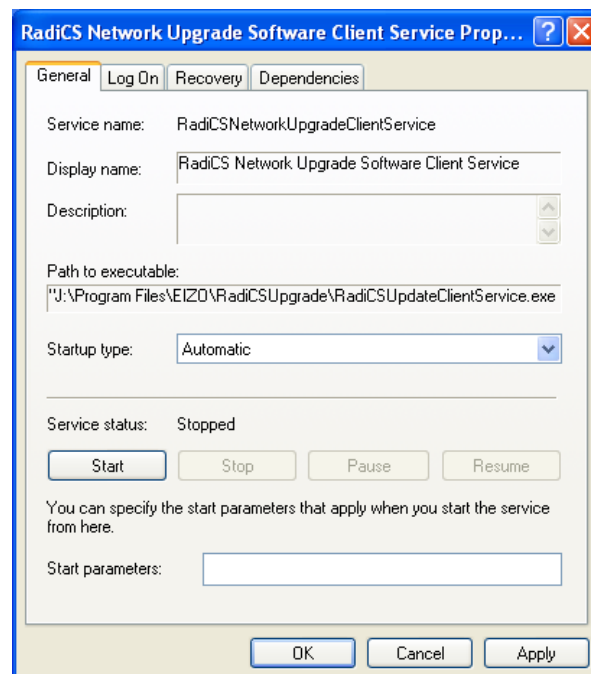




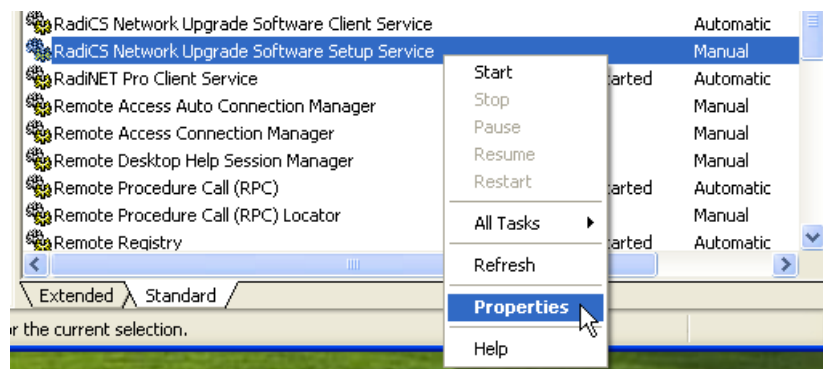
- 3. Click the right mouse button on “RadiCS Network Upgrade Software Client Service” and select [Properties].**



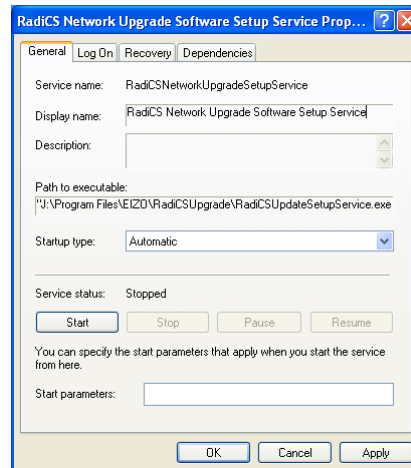
- 4. The “RadiCS Network Upgrade Software Client Service Properties” screen appears. Select “Automatic” in “Startup type” of “General” tab. After entering the information, click [OK].**



- 5. Click the right mouse button on “RadiCS Network Upgrade Software Setup Service” and select [Properties].**

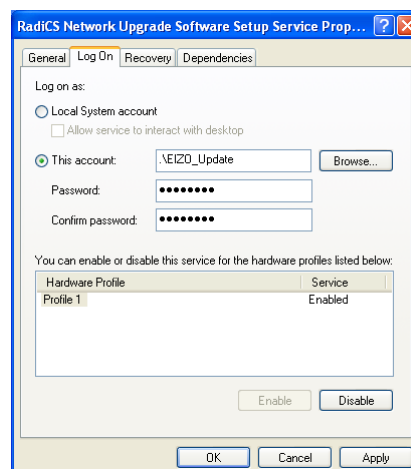


- 6.** The “RadiCS Network Upgrade Software Setup Service Properties” screen appears. Select “Automatic” in “Startup type” of “General” tab. After entering the information, select “Logon” tab.

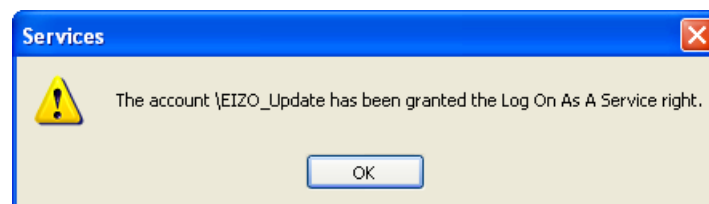


- 7.** Select “This account” in “Log on as:” of “Log On” tab. Set the following and then click [OK].

- This account: Enter the user name created in “6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 42) or “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71)
- Password: Enter password for the account
- Confirm password: Enter password same as “Password”



- 8.** The message “The account xxxxxx has been granted the Log On As A Service right.” is displayed. Click [OK].

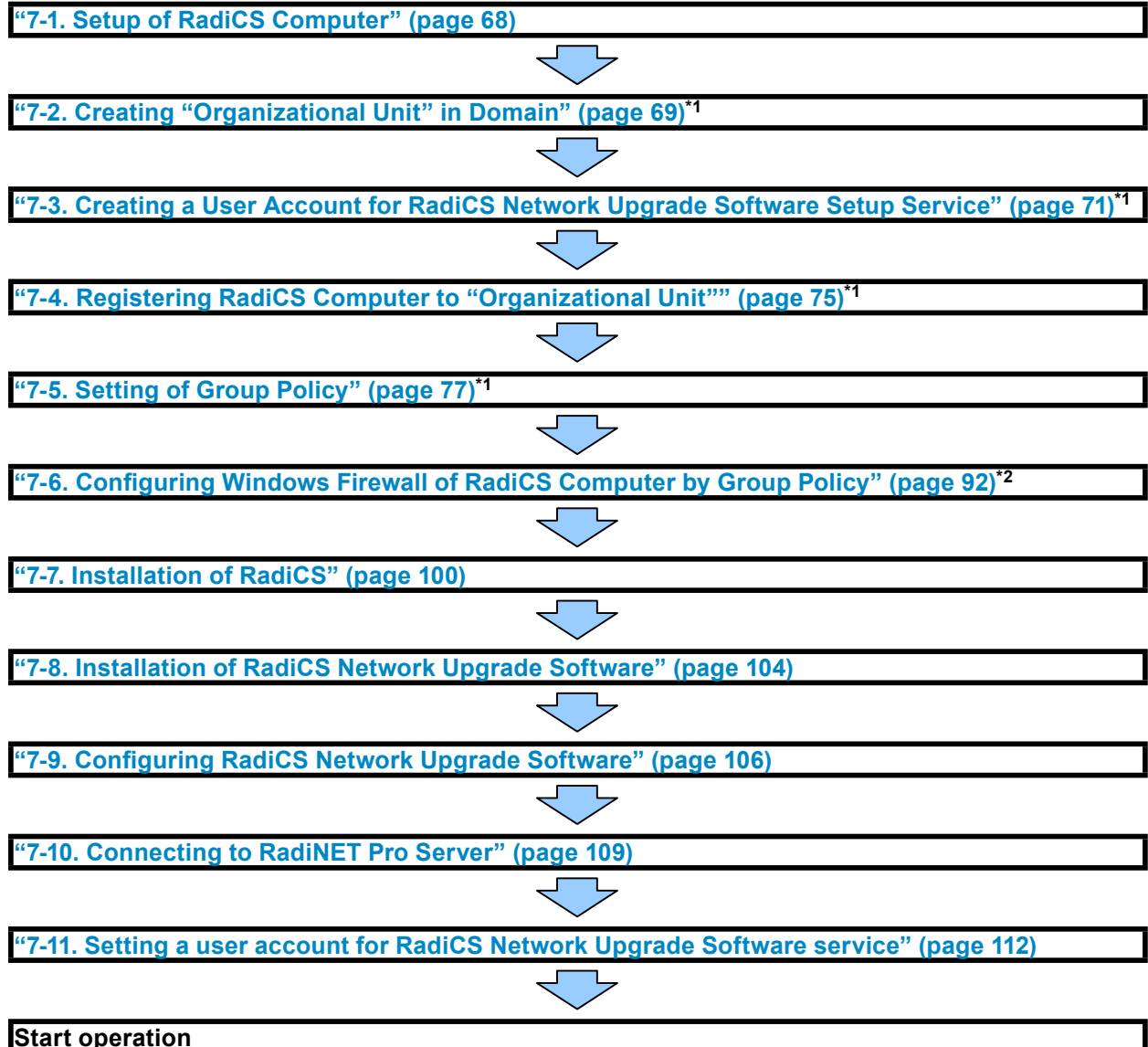


# Chapter 7 Setup of RadiCS Computer (DOMAIN)

## DOMAIN

A server called “domain controller” exclusively manages all the users and resources in the domain. As long as computers within the domain are used, the users are managed by the domain controller. Therefore, each computer does not have to manage its users. The domain option is suitable for creating a large-scale network.

The setup flow of RadiCS computer (DOMAIN) is the following.



\*1 Operate on the domain server.

\*2 If the Windows firewall function is active during the installation of RadiCS, communication with a required program will be enabled. If you need to configure Windows Firewall manually, refer to “7-6. Configuring Windows Firewall of RadiCS Computer by Group Policy” (page 92).

## 7-1. Setup of RadiCS Computer

---

### Procedure

- 1. Prepare a suitable computer for RadiCS system requirements.**
- 2. Install the graphics card in the computer according to the installation manual supplied with the graphics card.**
- 3. Connect the EIZO Monitor and the computer with the signal cable and USB cable.**
- 4. Install the device driver of graphics card according to the installation manual supplied with the graphics card.**

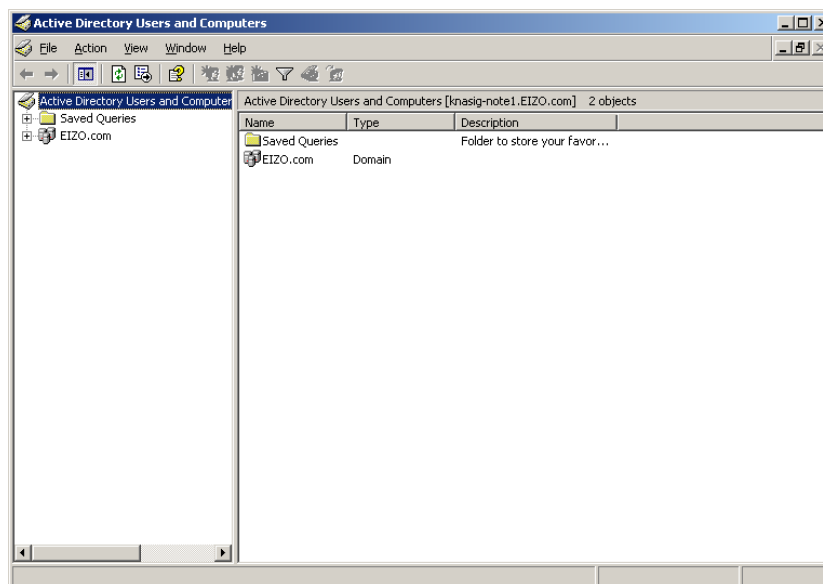
## 7-2. Creating “Organizational Unit” in Domain

- Steps “The setting of group policy” and “Configuring Windows Firewall” are required to enable communications between the RadiNET Pro server and the RadiCS computer. Create an “Organizational Unit” in order to configure the RadiCS computer for these settings.
- To manage more than one RadiCS computer in the domain, create an “Organizational Unit” where the RadiCS computers are registered.
- Security policies and Windows firewall are set by “Organizational Unit”.

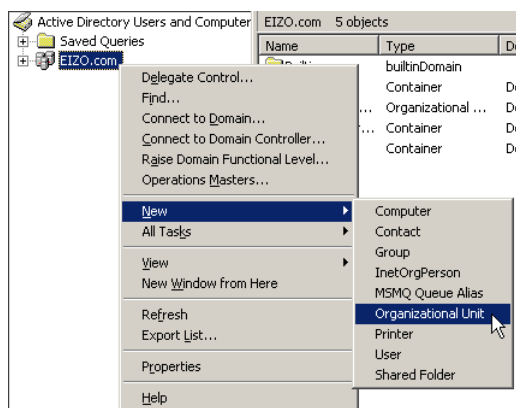
### ● For both Windows Server 2003 and Windows Server 2008

#### Procedure

1. Double click [Active Directory Users and Computers] from [Administrative Tools] in Windows.

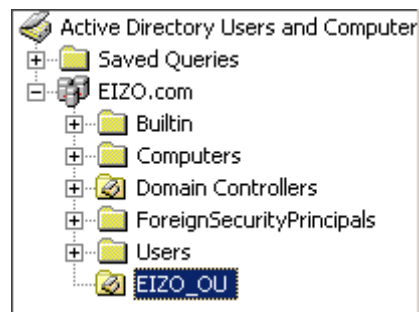


2. From the left side of the screen, select domain and then click the right mouse button. Select [New] - [Organizational Unit] from the menu.



3. The “New Object - Organizational Unit” screen appears. Enter the name of “Organizational Unit” to “Name” and then click [OK].

- 4.** The “Active Directory Users and Computers” screen reappears. The created “Organizational Unit” is displayed in the left side of the screen.



## 7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service

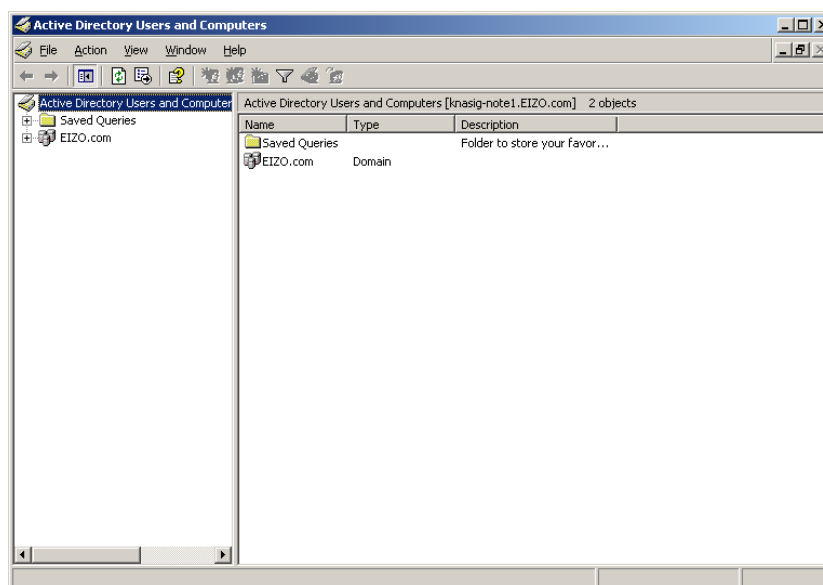
### Attention

- Before creating a user account, complete “7-2. Creating “Organizational Unit” in Domain” (page 69).
- Create a user account and add to “Domain Admins” group. Before creating user, notify to the administrator to create exclusive user.

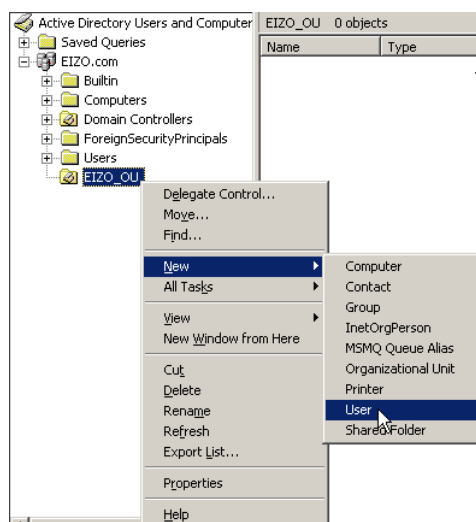
### ● For both Windows Server 2003 and Windows Server 2008

#### Procedure

1. Double click [Active Directory Users and Computers] from [Administrative Tools] in Windows.



2. Select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69) and click the right mouse button. Select [New] - [User] from the menu.



**3. The “New Object - User” screen appears. Set the following items and then click [Next].**

- First Name: Enter user name
- User logon name: Enter logon name to logon

New Object - User

Create in: EIZO.com/EIZO\_OU

First name: EIZO\_Update Initials:

Last name:

Full name: EIZO\_Update

User logon name: EIZO\_Update @EIZO.com

User logon name (pre-Windows 2000): EIZO\ EIZO\_Update

< Back Next > Cancel

**4. The password setup screen appears. Set the following items and then click [Next].**

- Password: Enter password to logon
- Confirm password: Enter password same as “Password”
- User must change password at next logon: No check
- User cannot change password: No check
- Password never expires: Check
- Account is disabled: No check

New Object - User

Create in: EIZO.com/EIZO\_OU

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

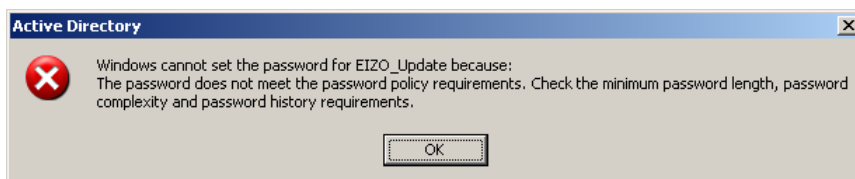
< Back Next > Cancel



---

**Note**

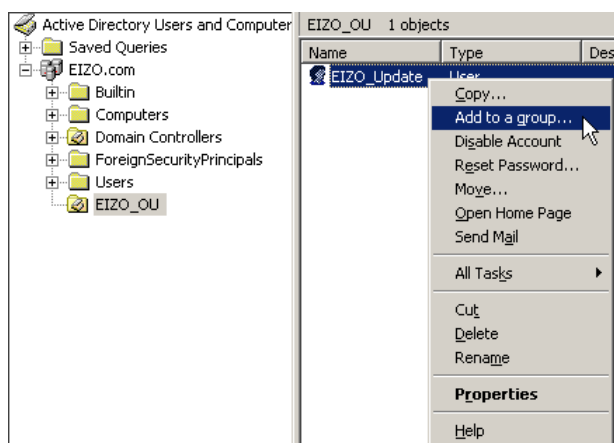
- The Windows policy may request a more complex password. If the user tries to set a password which does not conform to the policy, an “error message” will be displayed when the user clicks [Finish] in Step 5. In this case, go back to the password setup screen and set an appropriate password.

**Windows password policy**

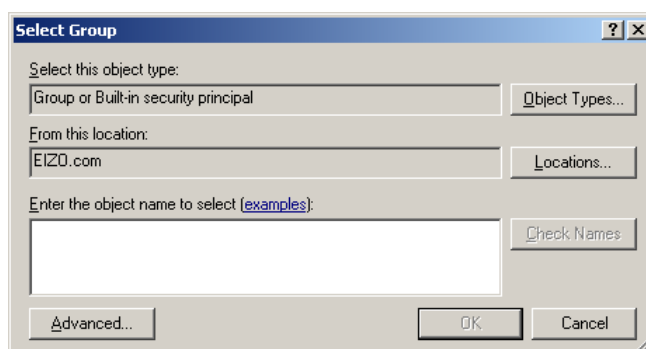
- Not contain user account name or most of your full name
  - Minimum password length must be 6 characters
  - Use the character with three categories out of four shown below.
    - English capital letter (A-Z)
    - English small letter (a - z)
    - Decimal number (0 - 9)
    - Non-alphabet character (!, \$, #, % etc.)
- 

**5. The confirmation password setup screen appears. Click [Finish].**

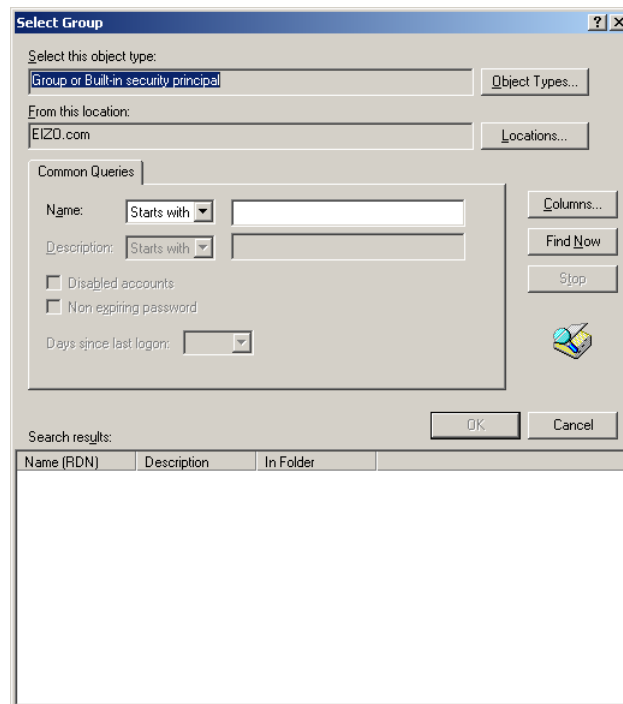
**6. The “Active Directory Users and Computers” screen reappears. The created user account is displayed in the right side of the screen. Select the user and click the right mouse button. Select [Add to a group...] from the menu.**



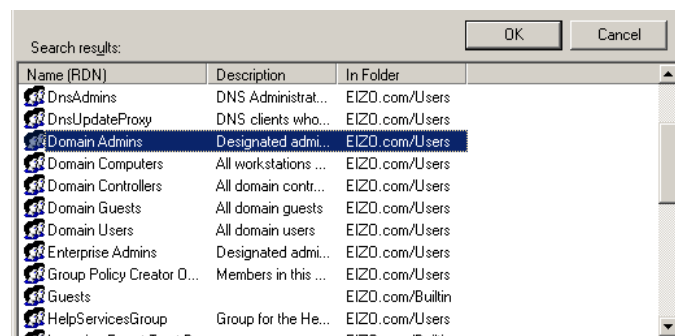
**7. The “Select Group” screen appears. Click [Advanced...].**



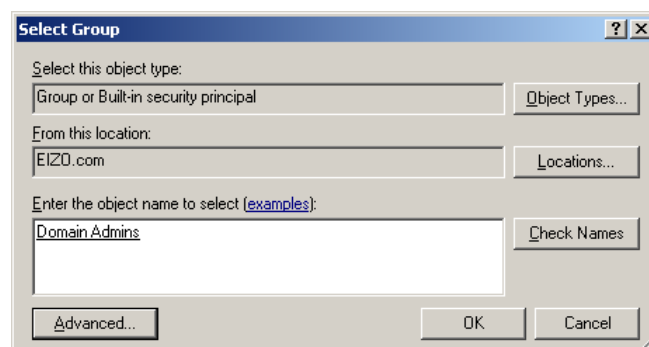
**8. The search screen appears. Click [Find Now].**



**9. “User name” and “Group name” are displayed in “Search results”. Select “Domain Admins” and then click [OK].**



**10. The “Select Group” screen reappears. Click [OK].**



**11. The message “The Add to Group operation was successfully completed.” is displayed. Click [OK].**

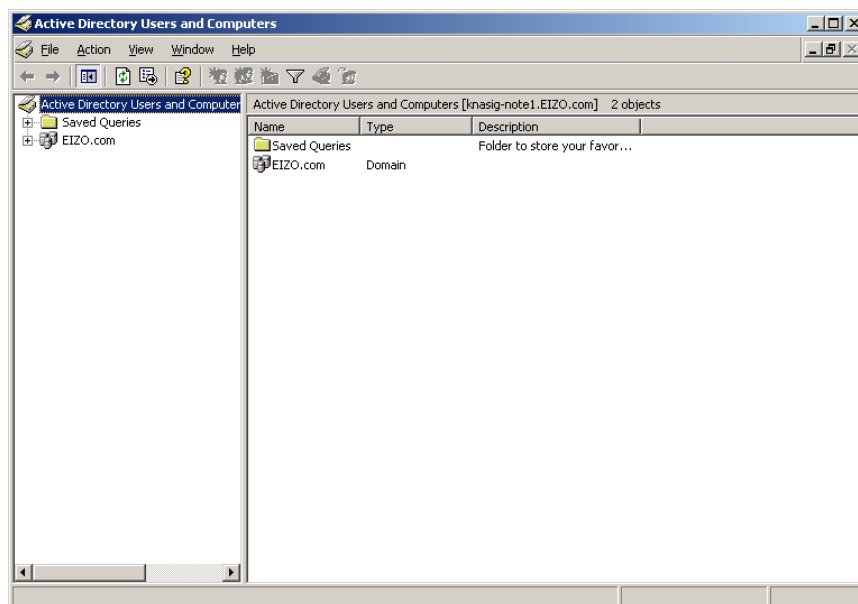
## 7-4. Registering RadiCS Computer to “Organizational Unit”

Registering RadiCS computer to “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69).

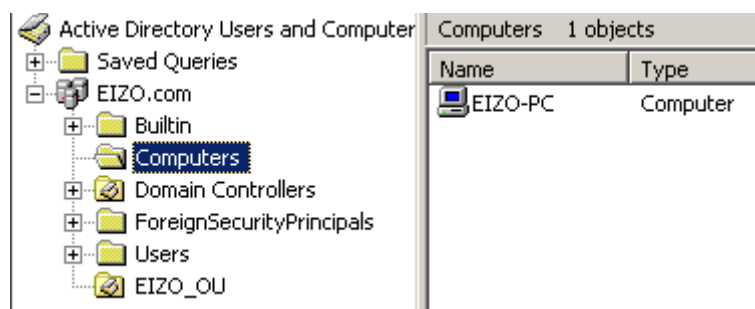
### ● For both Windows Server 2003 and Windows Server 2008

#### Procedure

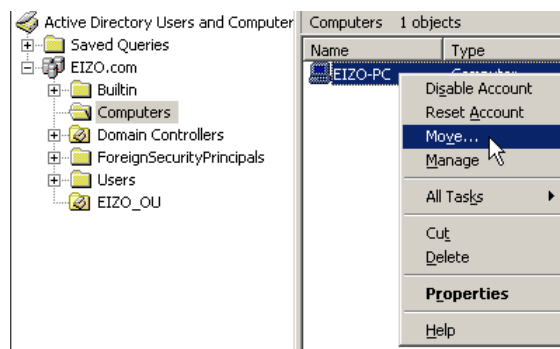
1. Select [Active Directory Users and Computer] from the [Administrative tools] in Windows.



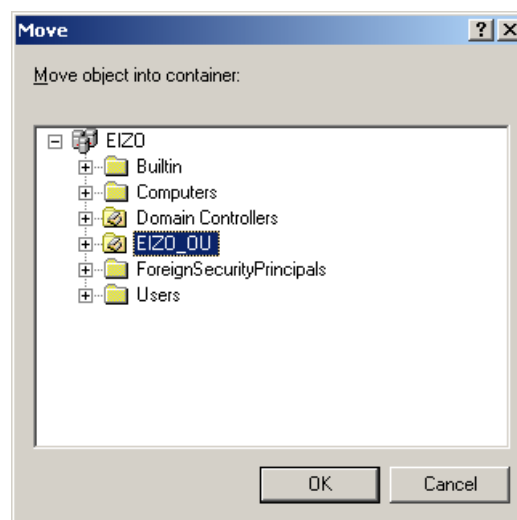
2. From the left side of the screen, select “Computers”. The computer in domain is displayed in the right side of the screen.



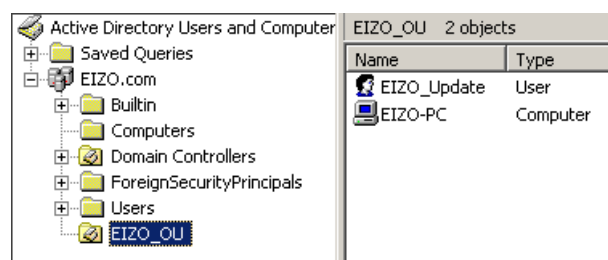
3. Click RadiCS computer from the left side of the screen and click the right mouse button. Select [Move...] from the menu.



4. The “Move” screen appears. Select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69) in Domain” and click [OK].



5. The “Active Directory Users and Computers” screen reappears. From the left side of the screen, select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69). RadiCS computer moved to “Organizational Unit” is displayed in the right side of the screen. Similarly, register all RadiCS computer to “Organizational Unit”.



## 7-5. Setting of Group Policy

If you use Windows Server 2008 on the domain controller, refer to “For Windows Server 2008” (page 85).

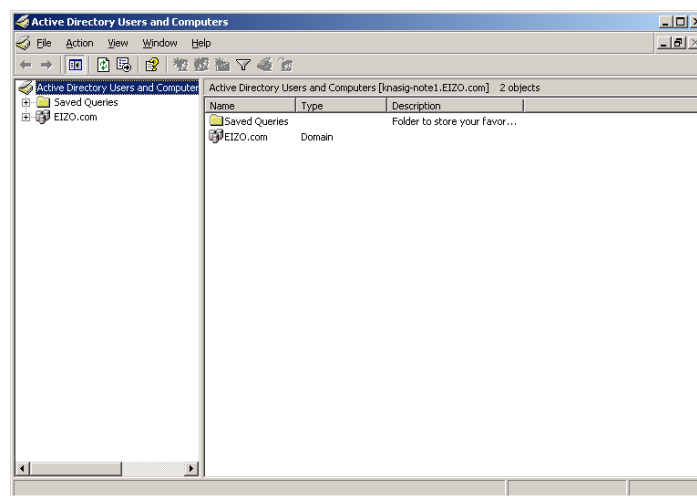
### Attention

- Assign the “Log on as a service” authority for the computer on which the service is running. RadiCS Network Upgrade Software service cannot be started without the authority.
- Set “Deny log on locally” to the computer on which the service is running. This will prevent the created “Domain user” from logging on to Windows.

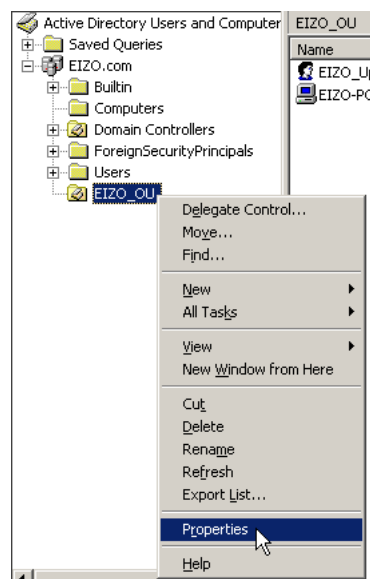
## ● For Windows Server 2003

### Procedure

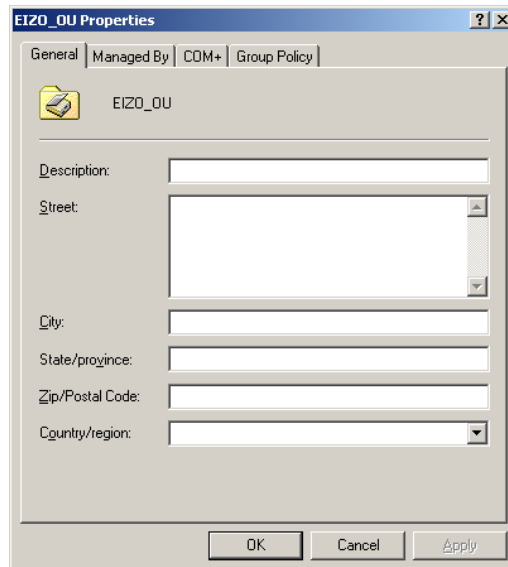
1. Double click [Active Directory Users and Computers] from [Administrative Tools] in Windows.



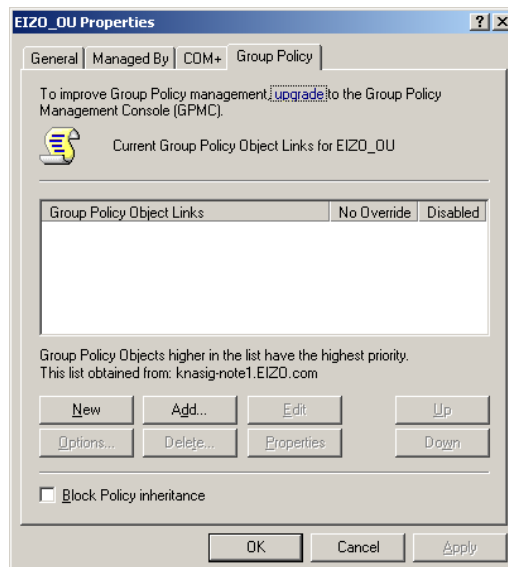
2. From the left side of the screen, select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69) in Domain” and click the right mouse button. Select [Properties] from the menu.



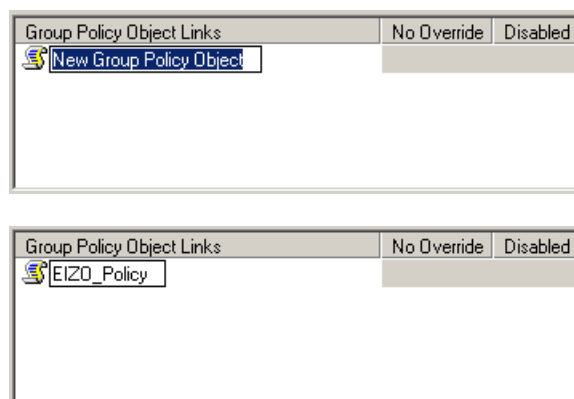
**3. The “Properties” screen appears. Select the “Group Policy” tab.**



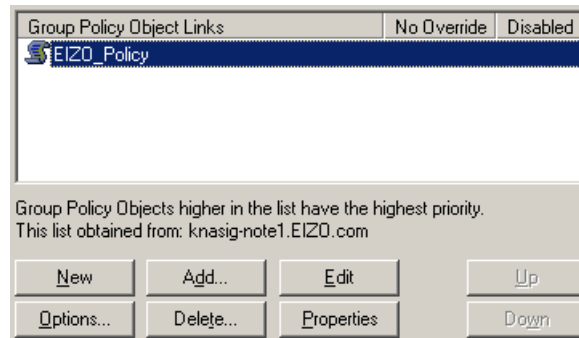
**4. The “Group Policy” tab is displayed. Click [New].**



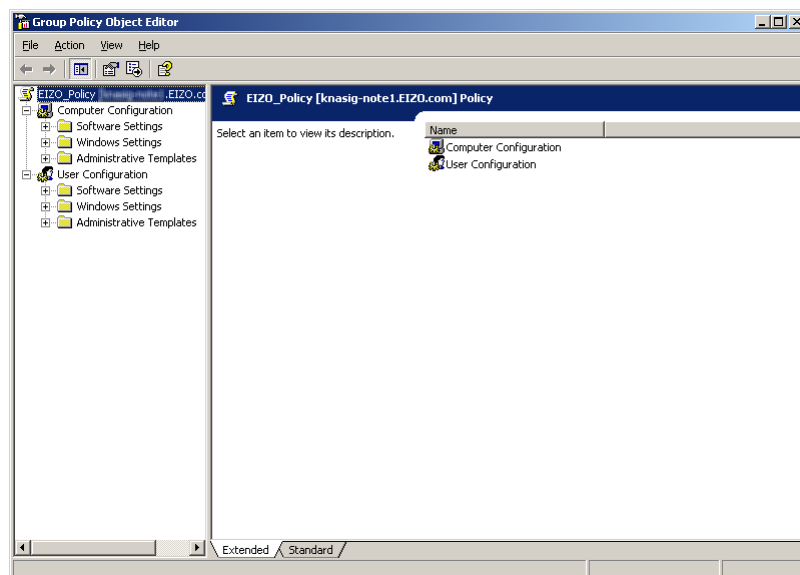
**5. The “New Group Policy Object” is displayed in the list. Change it to appropriate name.**



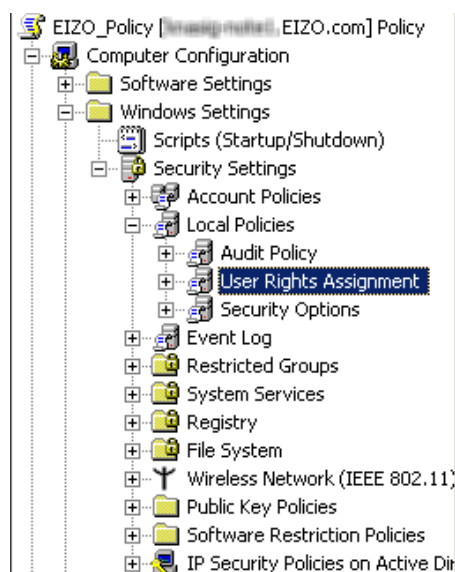
**6. Select the created “Group Policy Object” and then click [Edit].**



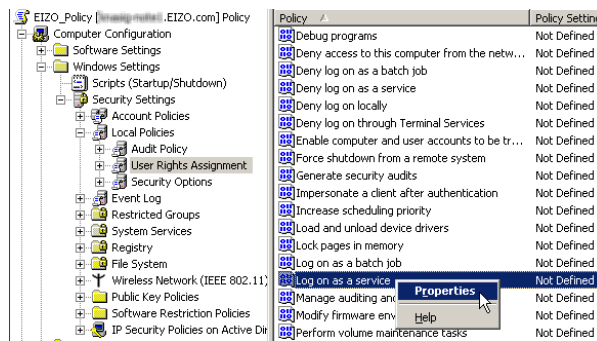
**7. The “Group Policy Object Editor” screen appears.**



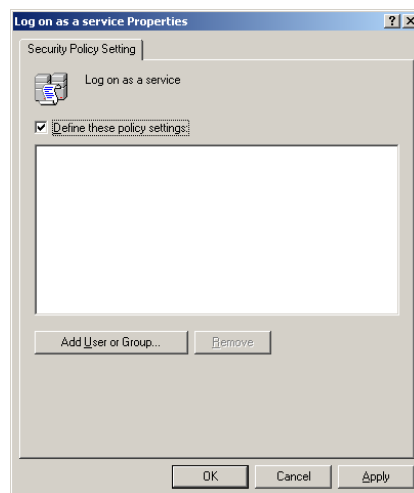
**8. From the left side of the screen, select “Computer Configuration” - “Windows Settings” - “Security Settings” - “Local Policies” - “User Rights Assignment”.**



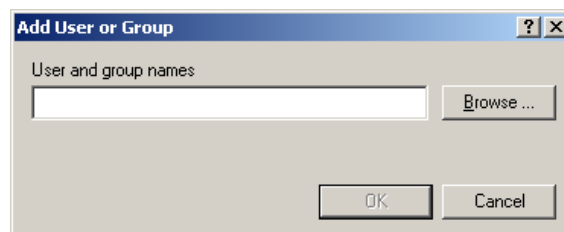
9. From the right side of the screen, select “Log on as a service” and click the right mouse button. Select [Properties] from the menu.



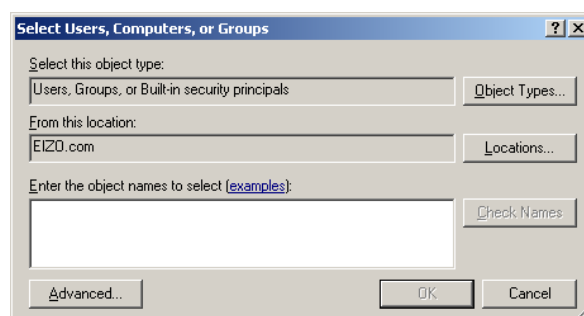
10. The “Log on as a service Properties” screen appears. Select “Define these policy settings” and then click [Add User or Group...].



11. The “Add User or Group” screen appears. Click [Browse...].

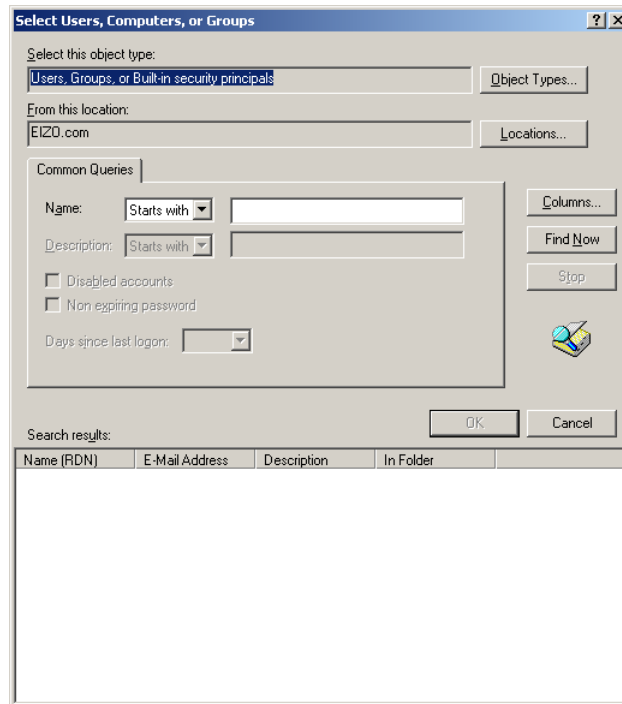


12. The “Select Users, Computers, or Groups” screen appears. Click [Advanced...].

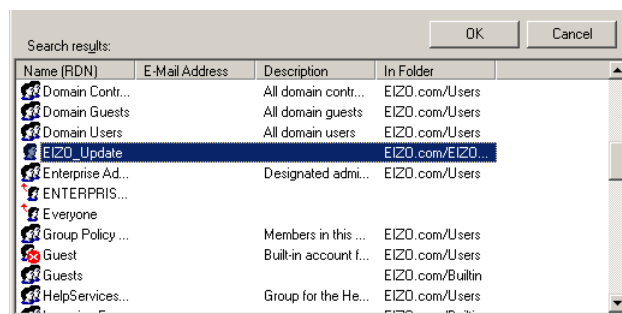




**13.** The search screen appears. Click [Find Now].



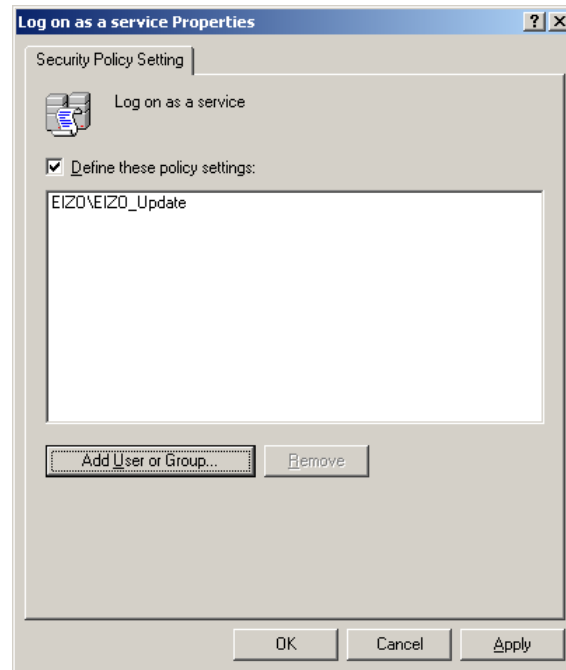
**14.** “User name” and “Group name” are displayed in “Search results”. Select the user created in “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71) and click [OK].



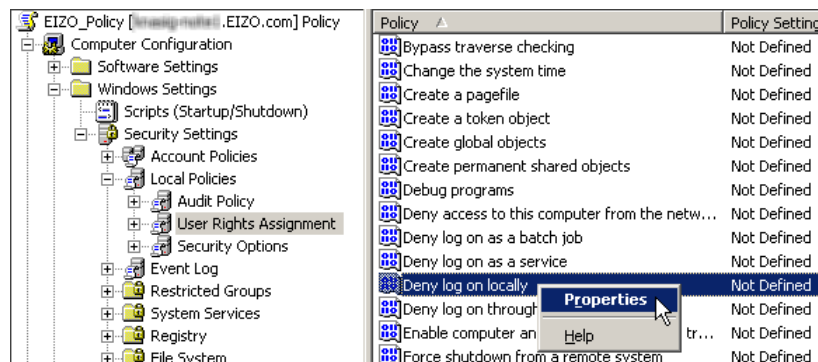
**15.** The “Select Users, Computers, or Group” screen reappears. Click [OK].

**16.** The “Add User or Group” screen reappears. Click [OK].

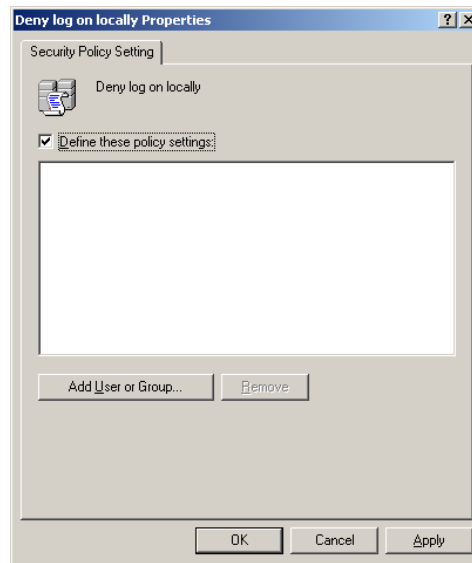
**17.** The “Log on as a service Properties” screen reappears. Click [OK].



**18.** The “Group Policy Object Editor” screen reappears. From the right side of the window, select “Deny log on locally” and click the right mouse button. Select [Properties] from the menu.



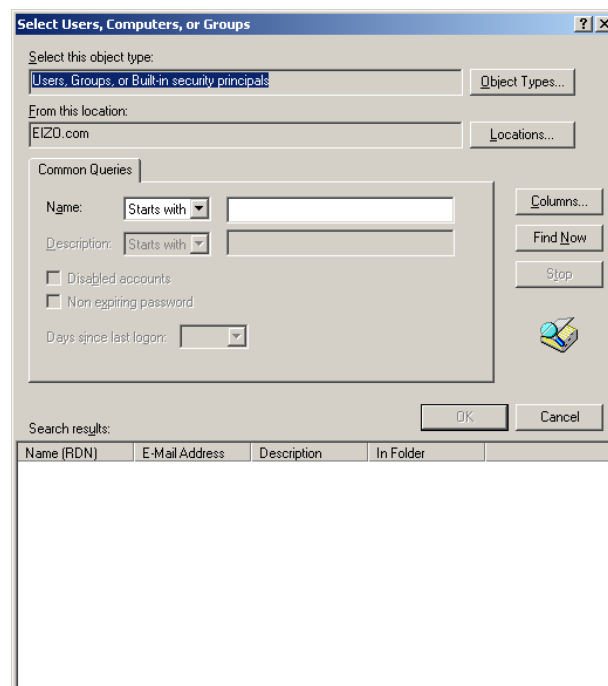
- 19.** The “Deny log on locally Properties” screen appears. Select “Define these policy settings” and then click [Add User or Group...].



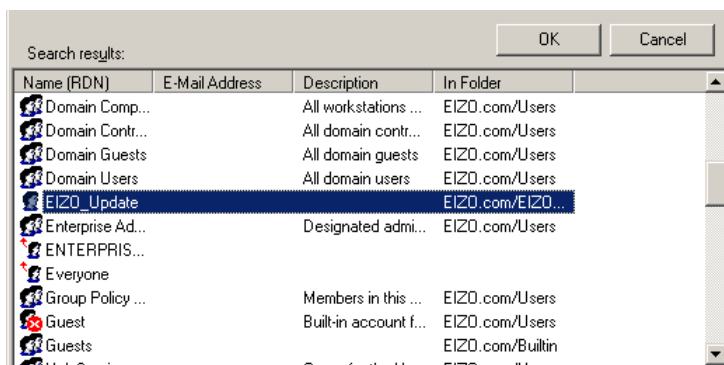
- 20.** The “Add User or Group” screen appears. Click [Browse...].

- 21.** The “Select Users, Computers, or Groups” screen appears. Click [Advanced...].

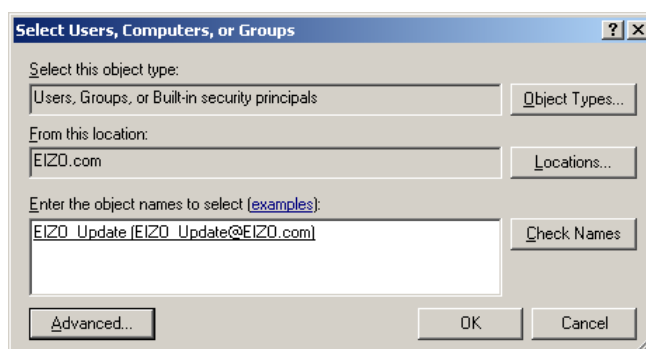
- 22.** The search screen appears. Click [Find Now].



**23.** “User name” and “Group name” are displayed in “Search results”. Select the user created in “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71) and click [OK].

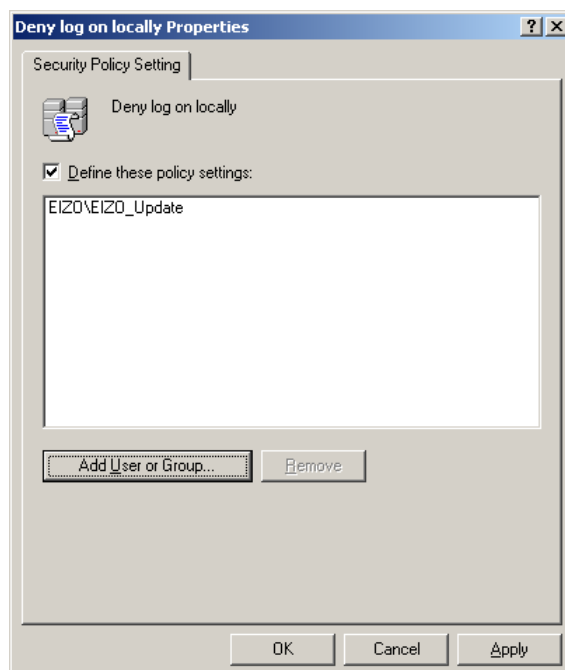


**24.** The “Select Users, Computers, or Groups” screen reappears. Click [OK].



**25.** The “Add User or Group” screen reappears. Click [OK].

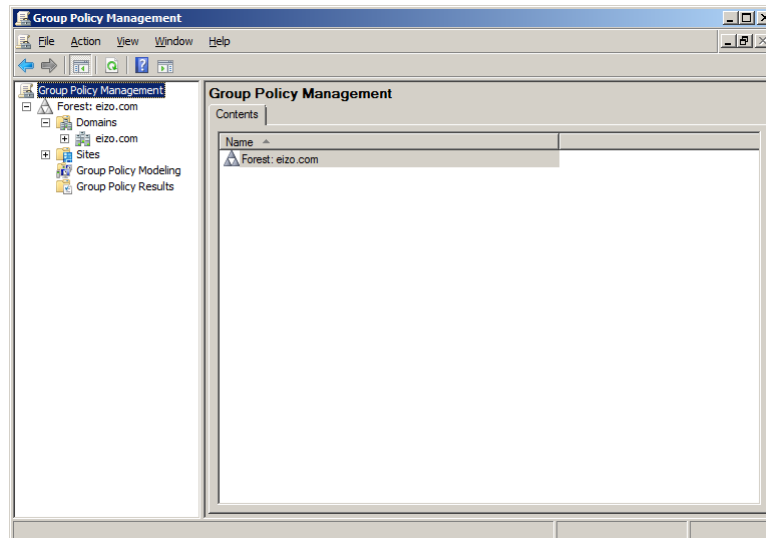
**26.** The “Deny log on locally Properties” screen reappears. Click [OK].



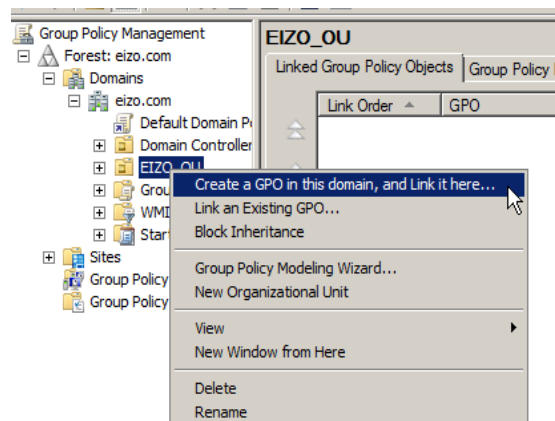
## ● For Windows Server 2008

### Procedure

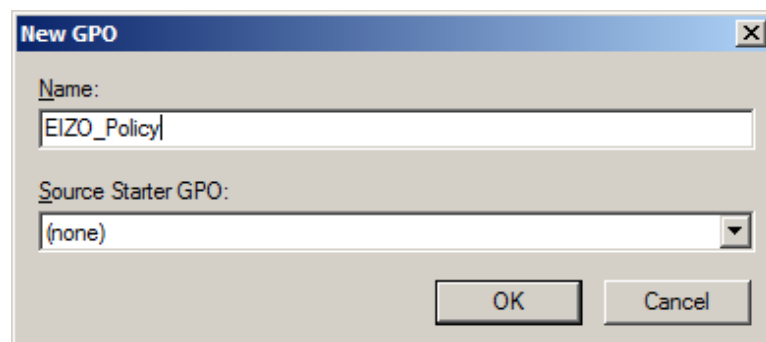
#### 1. Select [Group Policy Management] from [Administrative Tools] in Windows.



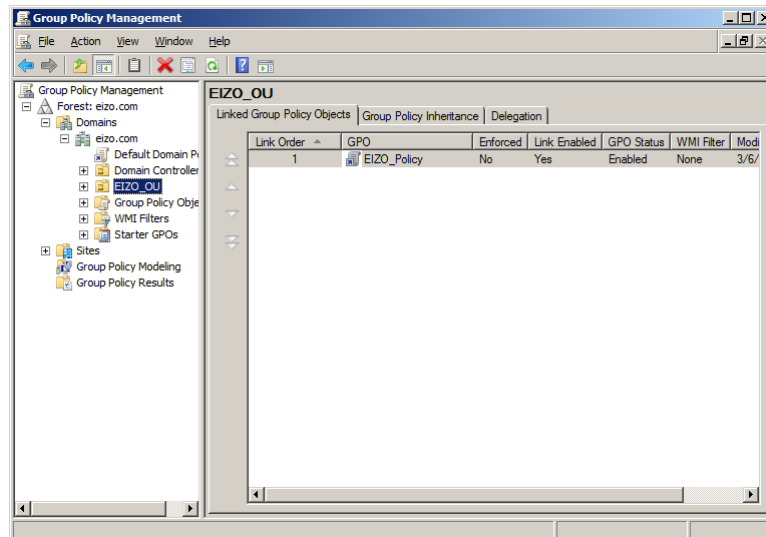
#### 2. Select the domain from the left side of the screen. Select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69) and click the right mouse button. Select [Create a GPO in this domain, and Link it here] from the menu.



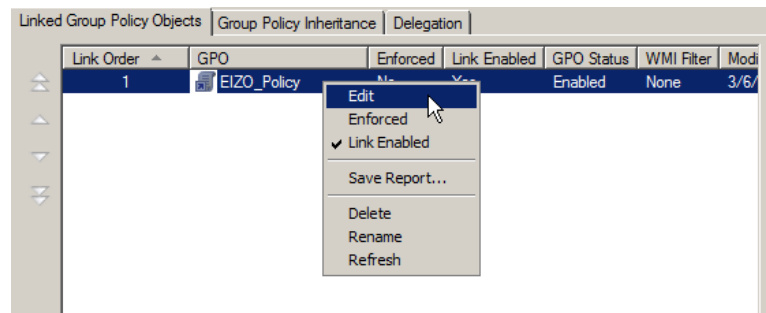
#### 3. The “New GPO” screen appears. Enter an appropriate name.



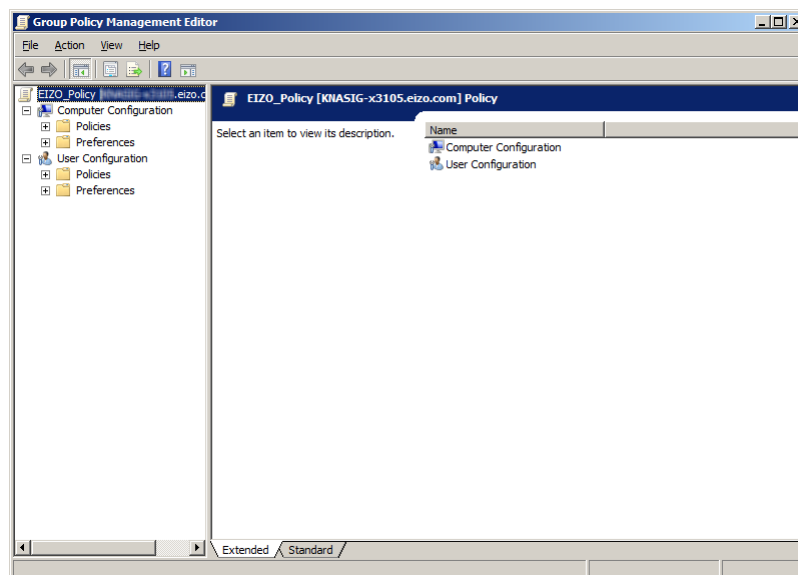
#### 4. A group policy object is created.



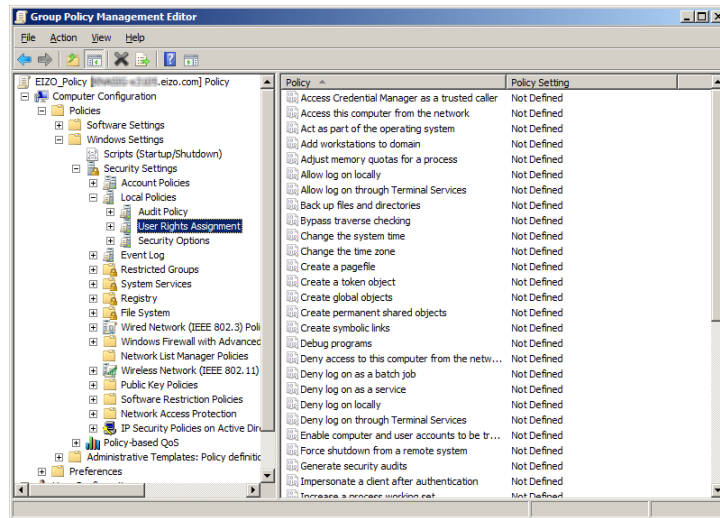
#### 5. Click the right mouse button on the created group policy object and select [Edit] from the menu.



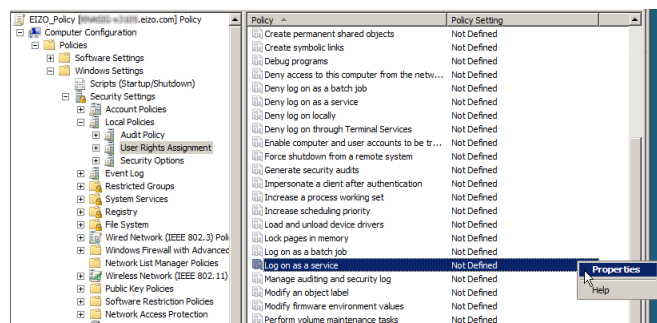
#### 6. The “Group Policy Management Editor” screen appears.



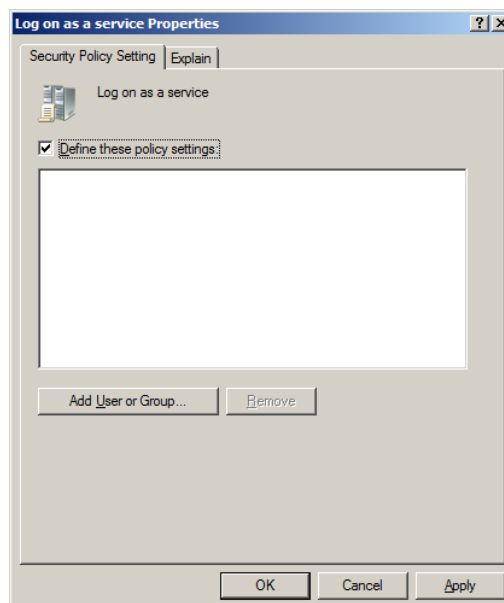
7. From the left side of the screen, select “Computer Configuration” - “Policies” - “Windows Settings” - “Security Settings” - “Local Policies” - “User Rights Assignment”.



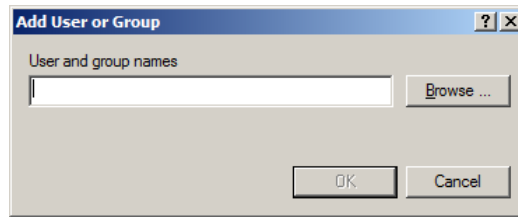
8. Select “Log on as a service” from the right side of the screen and click the right mouse button. Then select [Properties] from the menu.



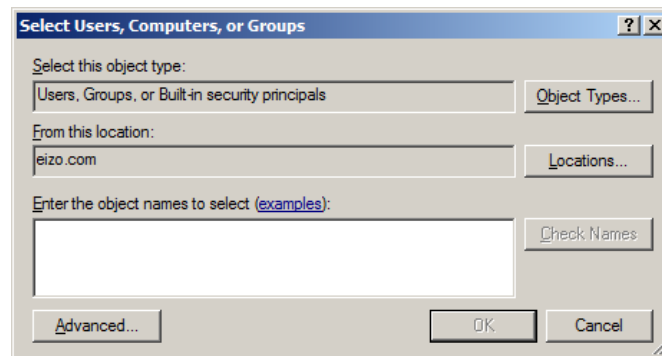
9. The “Log on as a service Properties” screen appears. Check the “Define these policy settings” checkbox and then click [Add User or Group...].



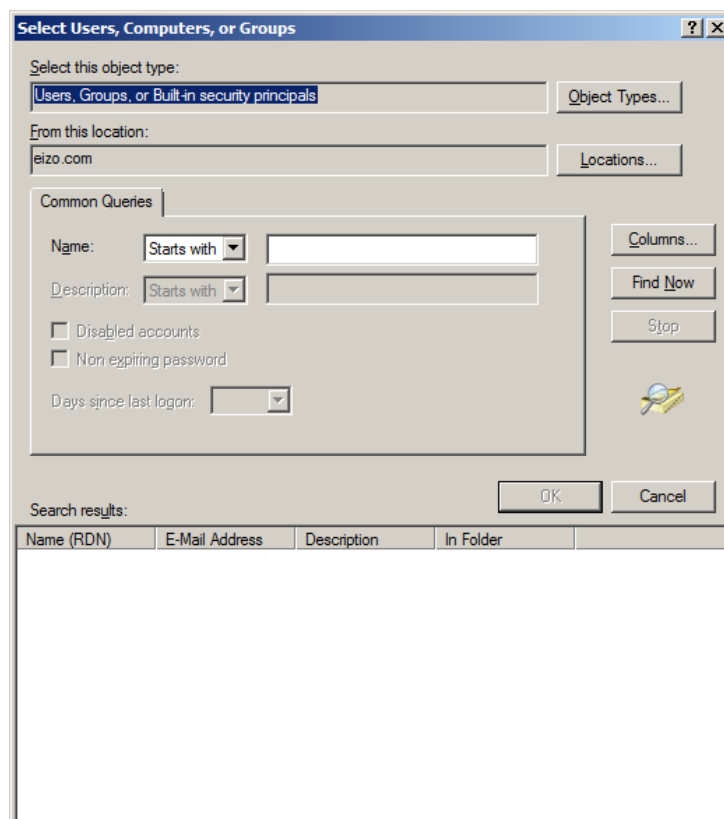
**10.** The “Add User or Group” screen appears. Click [Browse...].



**11.** The “Select Users, Computers, or Groups” screen appears. Click [Advanced...].

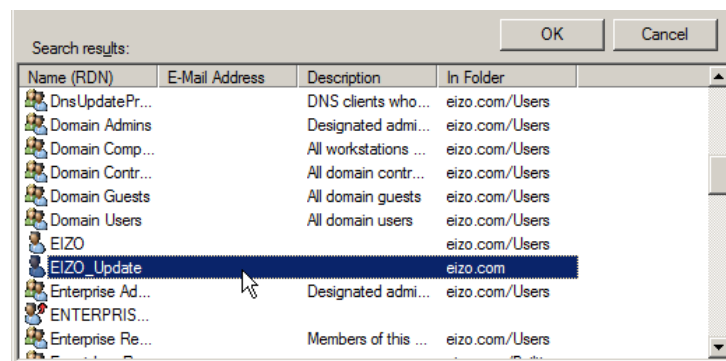


**12.** The search screen appears. Click [Find Now].





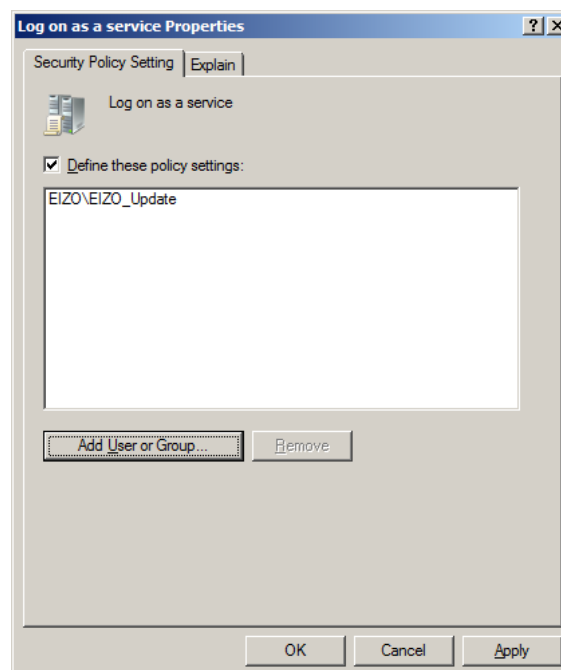
- 13.** “User name” and “Group name” are displayed in “Search results”. Select the user created in “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71) and click [OK].



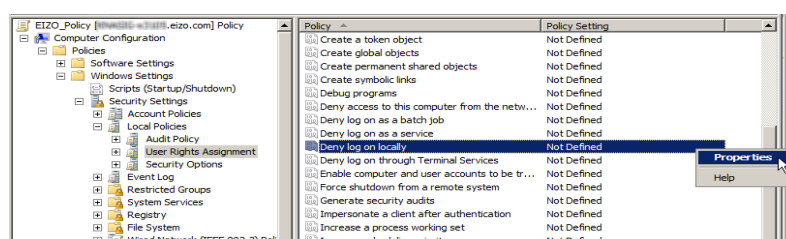
- 14.** The “Select Users, Computers, or Group” screen reappears. Click [OK].

- 15.** The “Add User or Group” screen reappears. Click [OK].

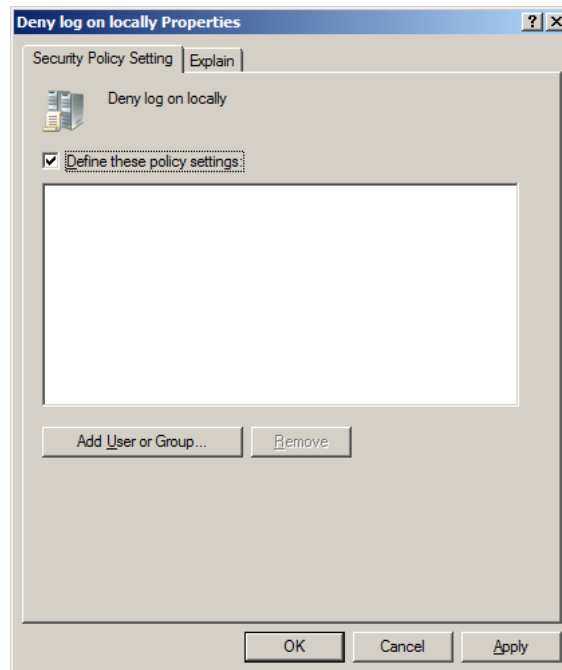
- 16.** The “Log on as a service Properties” screen reappears. Click [OK].



- 17.** The “Group Policy Management Editor” screen reappears. Select “Deny log on locally” from the right side of the screen and click the right mouse button. Then select [Properties] from the menu.



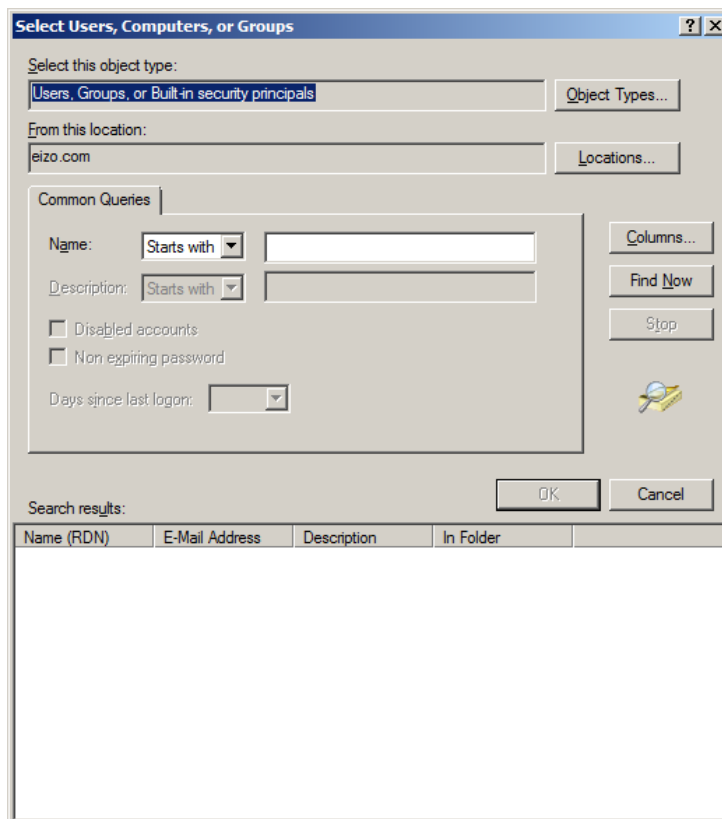
- 18.** The “Deny log on locally Properties” screen appears. Check the “Define these policy settings” checkbox and then click [Add User or Group...].



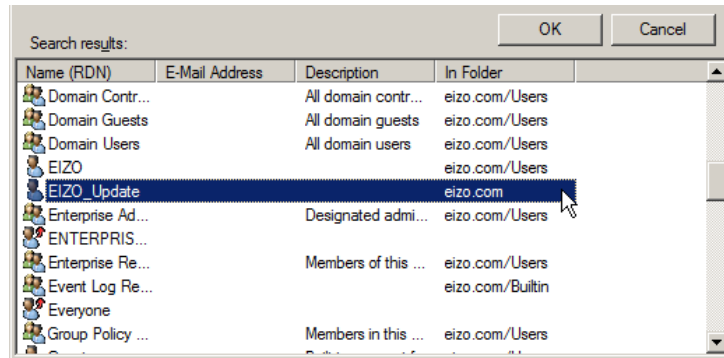
- 19.** The “Add User or Group” screen appears. Click [Browse...].

- 20.** The “Select Users, Computers, or Groups” screen appears. Click [Advanced...].

- 21.** The search screen appears. Click [Find Now].



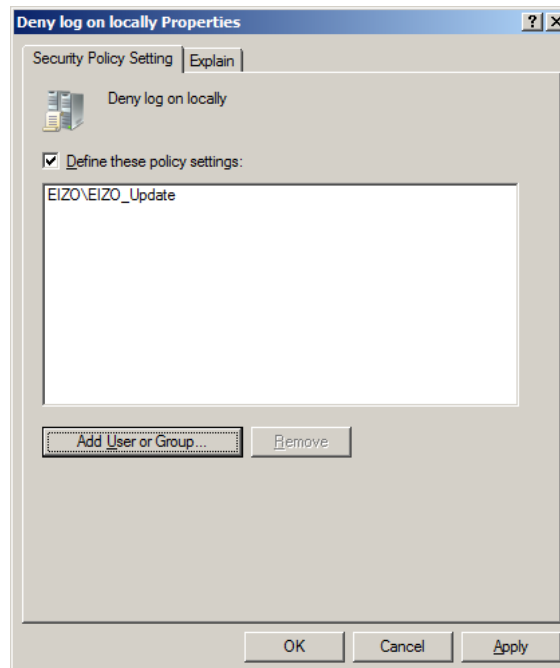
- 22.** “User name” and “Group name” are displayed in “Search results”. Select the user created in “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71) and click [OK].



- 23.** The “Select Users, Computers, or Group” screen reappears. Click [OK].

- 24.** The “Add User or Group” screen reappears. Click [OK].

- 25.** The “Deny log on locally Properties” screen reappears. Click [OK].



## 7-6. Configuring Windows Firewall of RadiCS Computer by Group Policy

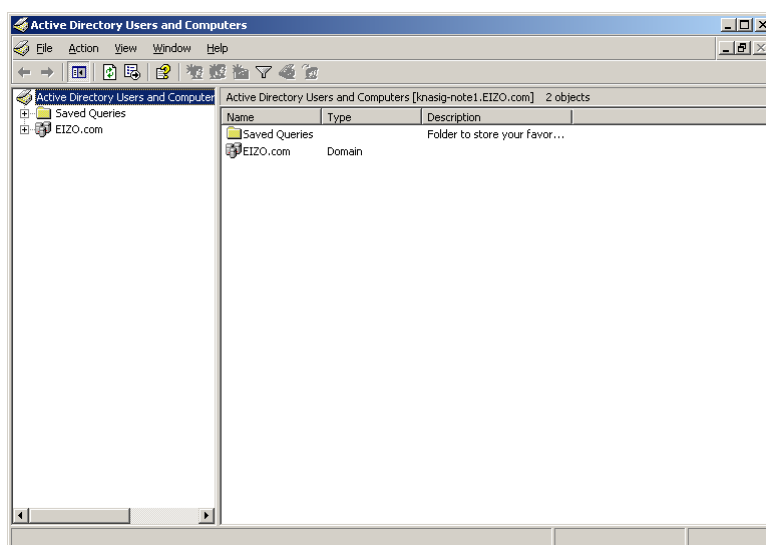
If you need to setup the Windows Firewall manually, perform the “Enable Program Communications” operations. Operate the following procedure on domain server.

### ● For Windows Server 2003

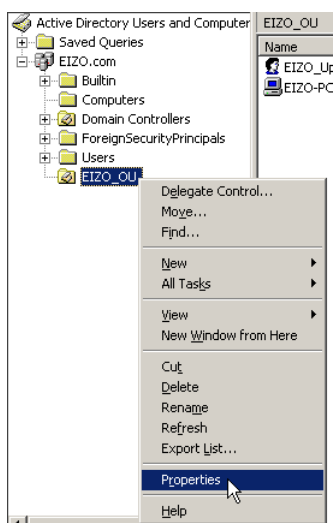
#### Enable Program Communications

#### Procedure

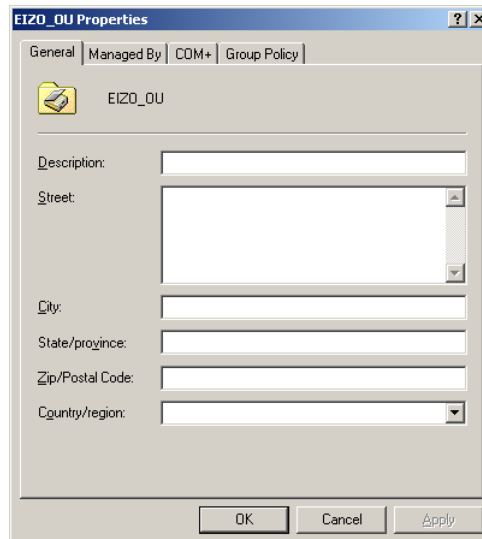
1. Select [Active Directory Users and Computer] from [Administrative tools] in Windows.



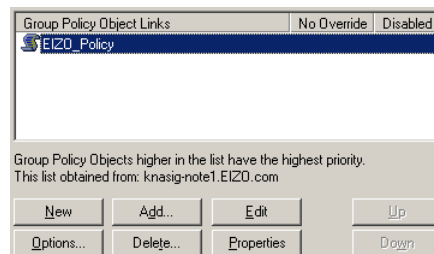
2. From the left side of the screen, select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69) and click the right mouse button. Select [Properties] from the menu.



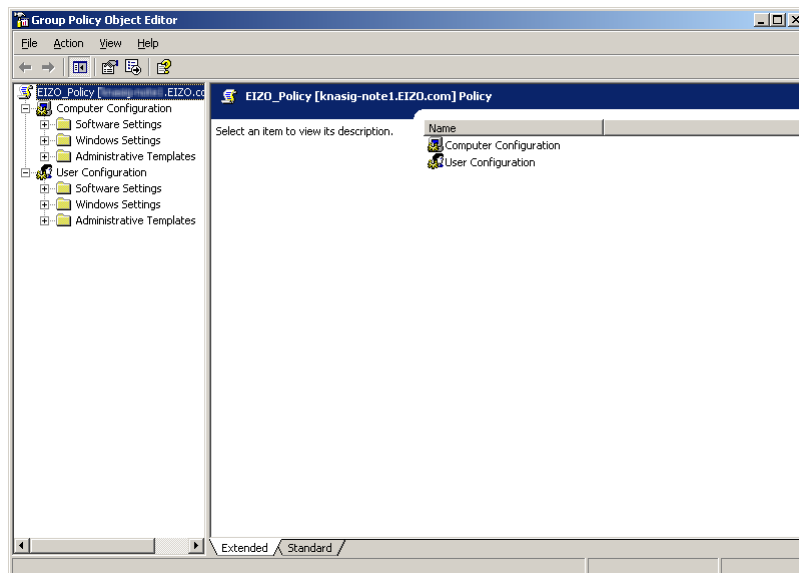
**3. The “Properties” screen appears. Select the “Group Policy” tab.**



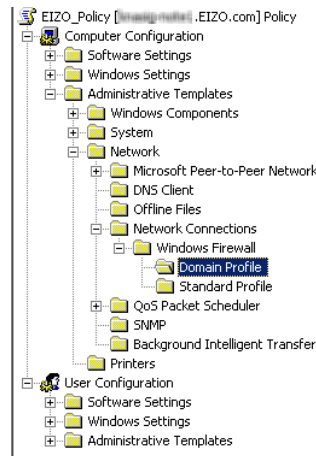
**4. Select “Group Policy Object” and click the [Edit].**



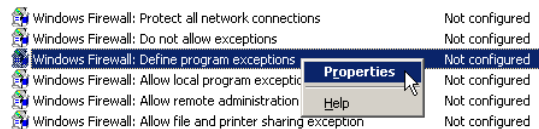
**5. The “Group Policy Object Editor” screen appears.**



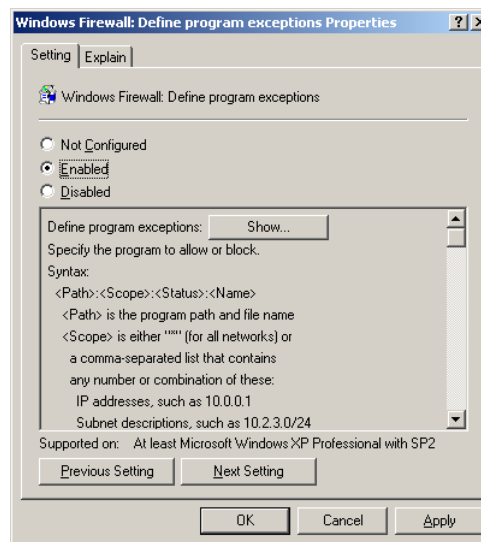
6. From the left side of the screen, select “Computer Configuration” - “Administrative Templates” - “Network” - “Network Connections” - “Windows Firewall” - “Domain Profile”.



7. From the right side of the screen, select “Define program exceptions” and then click the right mouse button. Select [Properties] from the menu.



8. “Windows Firewall: Define program exceptions Properties” screen appears. Select “Enabled” and click [Show...].



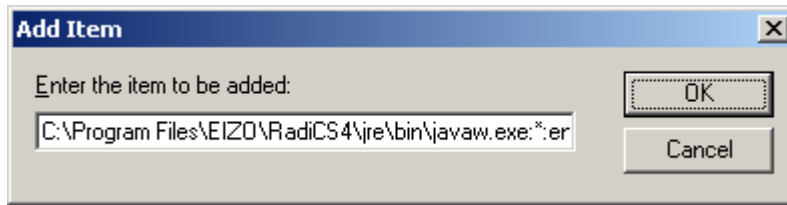
9. The “Show Contents” screen appears. Click [Add...].

## 10. The “Add Item” screen appears. Enter the following items.

### Attention

- Set a group policy suitable for each RadiCS computer if the installation drive is different.

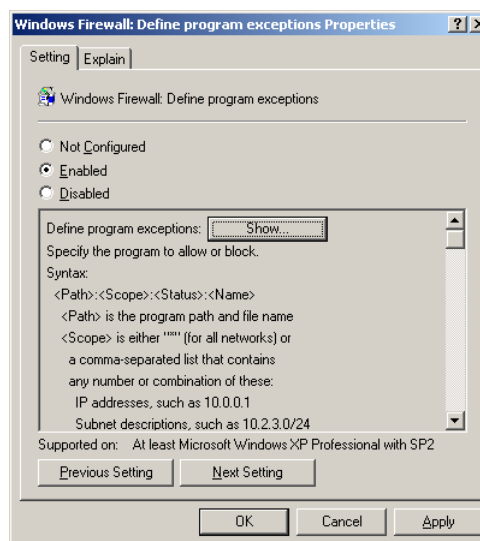
- Define javaw.exe exception  
(ex. C:\Program Files\EIZO\RadiCS4\jre\bin\javaw.exe:\*:enabled:RadiCS)



- Define “RadiCSUpdateClientService.exe” exception  
[Install folder]:\*:enabled: [applicable name]  
(ex. C:\Program Files\EIZO\RadiCSUpgrade\RadiCSUpdateClientService.exe:\*:enabled:RadiCSUpgradeClientService)

## 11. After the exception is defined, the added items appear in “Show Contents” screen. Click [OK].

## 12. The “Windows Firewall: Define program exceptions Properties” screen reappears. Click [OK].



## 13. The “Group Policy Object Editor” screen reappears. “Windows Firewall Define program exceptions Properties” in the right side of the screen is set to “Enable”.

## ● Windows Server 2008 / 2008 R2

### Allow Use of Communication Ports

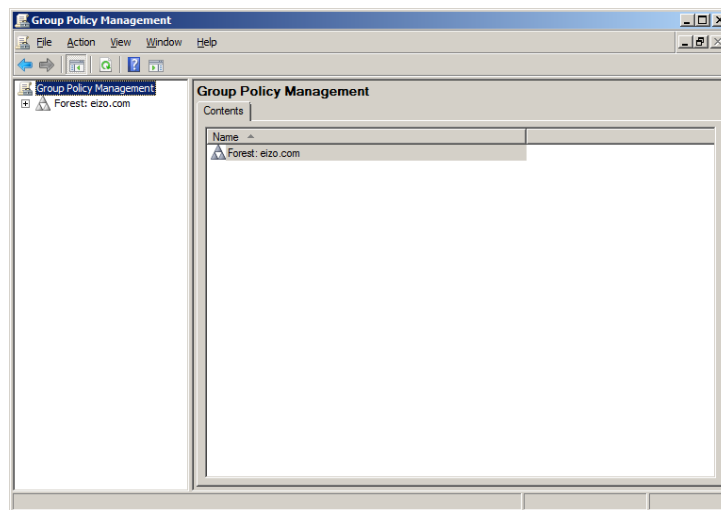
The following two programs are set.

- javaw.exe
  - C:\Program Files\EIZO\RadiCS4\jre\bin\javaw.exe
- RadiCSUpdateClientService.exe
  - C:\Program Files\EIZO\RadiCSUpgrade\RadiCSUpdateClientService.exe

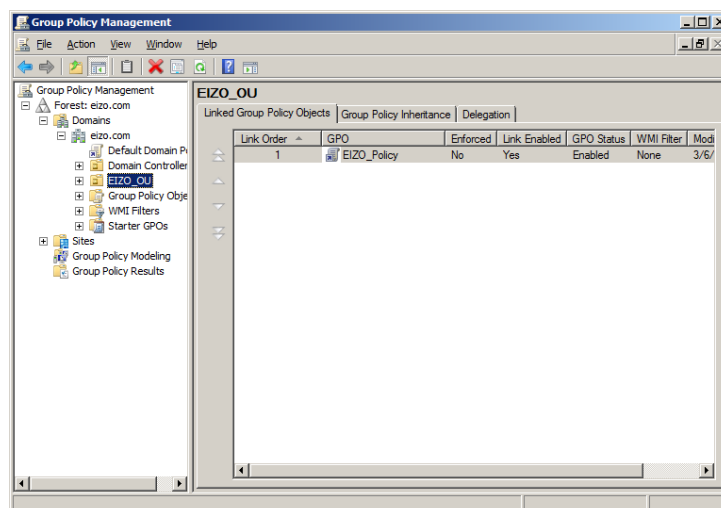
This section explains the setting procedure of javaw.exe.

### Procedure

#### 1. Select [Group Policy Management] from [Administrative Tools] in Windows.

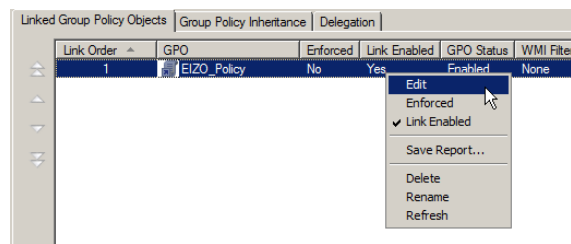


#### 2. Select the domain from the left side of the screen. Select “Organizational Unit” created in “7-2. Creating “Organizational Unit” in Domain” (page 69).

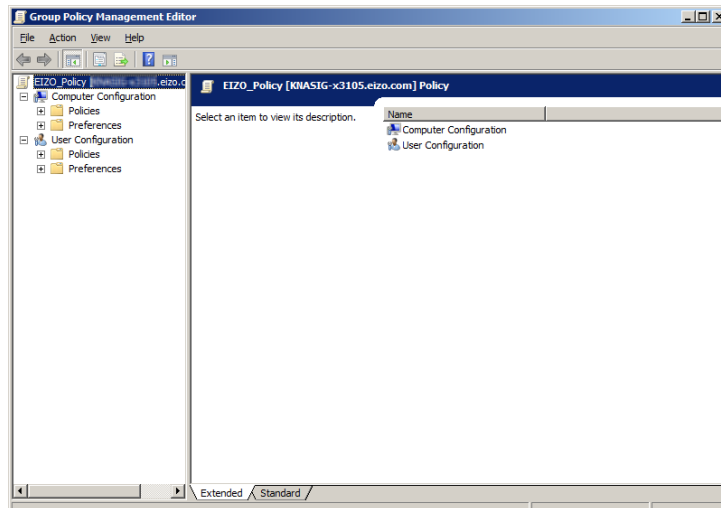




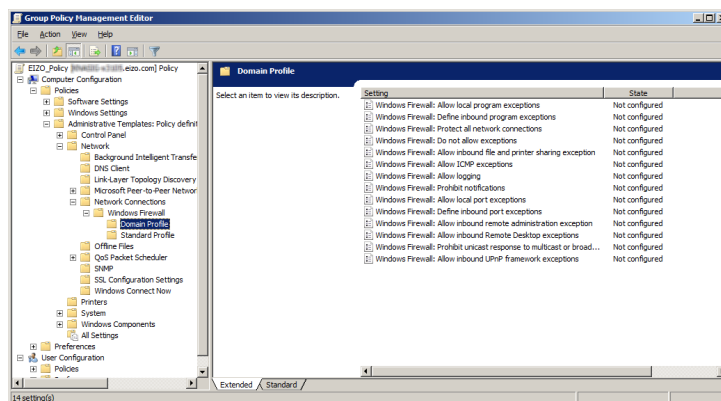
3. Click the right mouse button on the created group policy object and select [Edit] from the menu.



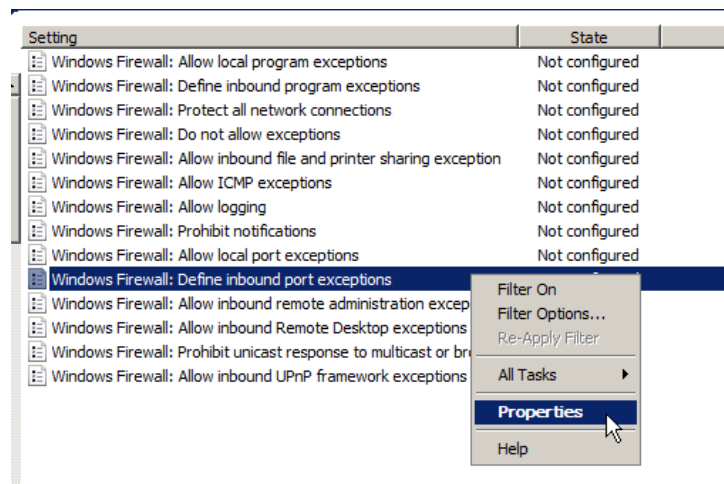
4. The “Group Policy Management Editor” screen appears.



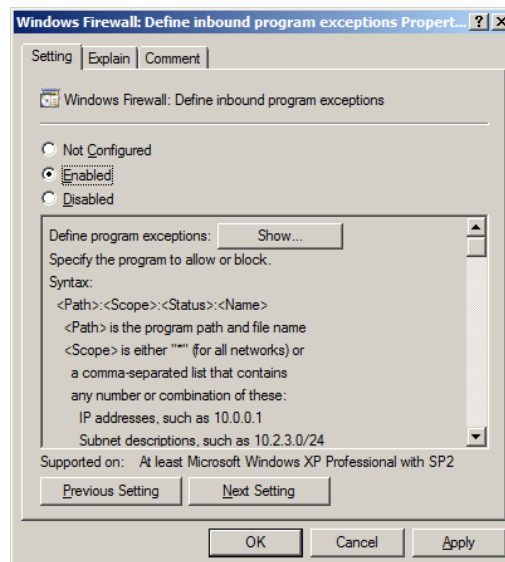
5. From the left side of the screen, select “Computer Configuration” - “Policies” - “Administrative Templates” - “Network” - “Network Connections” - “Windows Firewall” - “Domain Profile”.



- 6.** Select “Define inbound port exceptions” from the right side of the screen and click the right mouse button. Then select [Properties] from the menu.



- 7.** The “Windows Firewall: Define inbound program exceptions Properties” screen appears. Select “Enabled” and click [Show...].



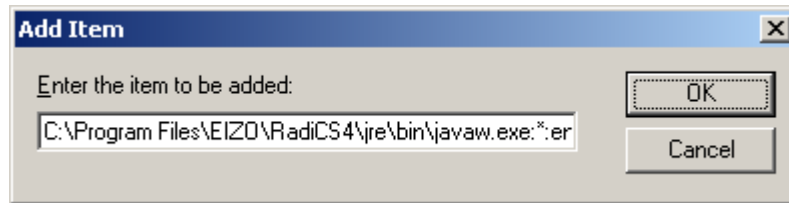
- 8.** The “Show Contents” screen appears. Click [Add...].

## 9. The “Add Item” screen appears. Enter the following items.

### Attention

- Set a group policy suitable for each RadiCS computer if the installation drive is different.

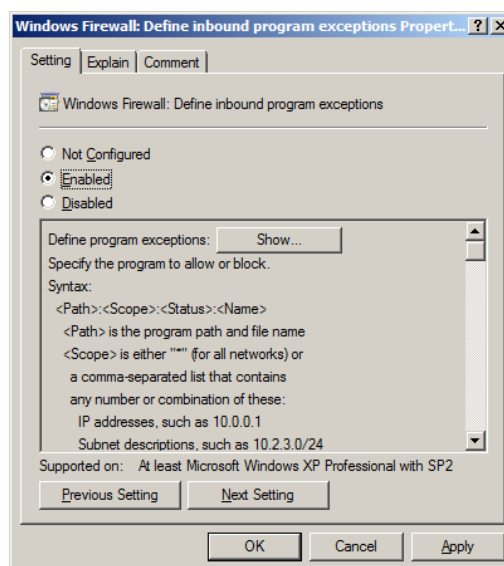
- Define javaw.exe exception  
(ex. C:\Program Files\EIZO\RadiCS4\jre\bin\javaw.exe:\*:enabled:RadiCS)



- Define “RadiCSUpdateClientService.exe” exception  
[Install folder]:\*:enabled: [applicable name]  
(ex. C:\Program Files\EIZO\RadiCSUpgrade\RadiCSUpdateClientService.exe:\*:enabled:RadiCSUpgradeClientService)

## 10. After the exceptions are defined, the added items appear in the “Show Contents” screen. Click [OK].

## 11. The “Windows Firewall: Define inbound port exceptions Properties” screen reappears. Click [OK].



## 12. The “Group Policy Management Editor” screen reappears. “Windows Firewall: Define inbound port exceptions” on the right side of the screen is set to “Enabled”.

## 7-7. Installation of RadiCS

---

The user account with administrator authority is required to install RadiCS.

---

**Note**

- “Windows Installer Ver.3.1” is installed automatically.
- 

### Procedure

- 1.** Insert the “RadiCS CD-ROM” to the drive and install RadiCS.
- 2.** The “EIZO RadiCS Setup” screen appears. Click “Install RadiCS”.

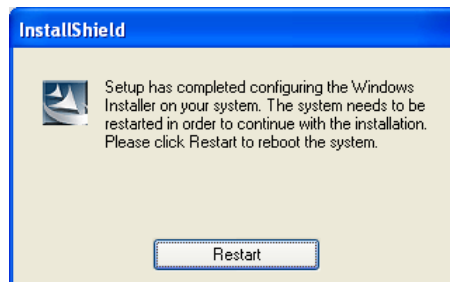


- 3.** You are prompted to restart the computer. Click [Restart].

---

**Note**

- No prompt to restart the computer appears on Windows Vista or Windows 7.



- 4.** After restarting Windows, “Open File - Security Warning” screen may appear. Click [Run].

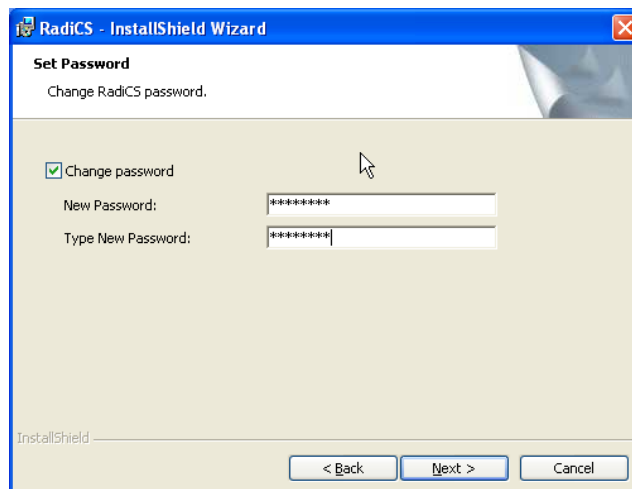


- 5.** The “RadiCS - InstallShield Wizard” screen appears. Click [Next].

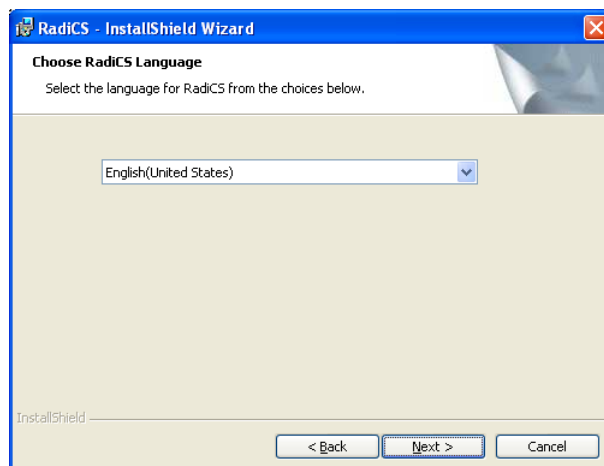


- 6.** The “License Agreement” screen appears. Select “I accept the terms in the license agreement” and then click [Next].

- 7.** The “Set Password” screen appears. Set password and then click [Next].  
Default password is “password”.

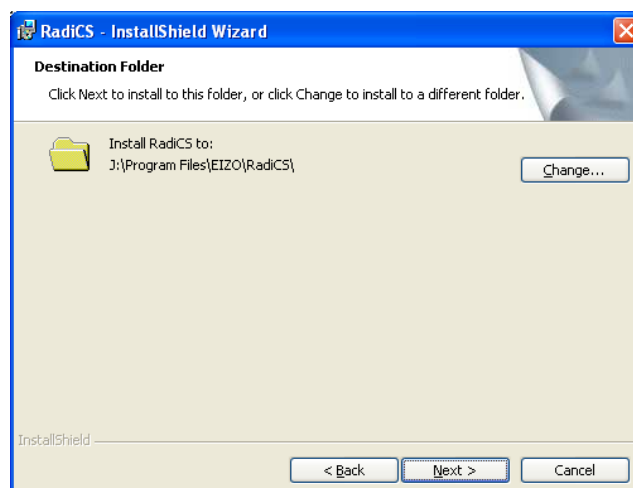


- 8.** The “Choose RadiCS Language” screen appears. Select the language and then click [Next].



- 9.** The “Destination Folder” screen appears. Click [Change...] if you change destination folder. Click [Next].

If you click [Change...], the “Change Current Destination Folder” screen appears. Specify the installation folder and then click [OK].

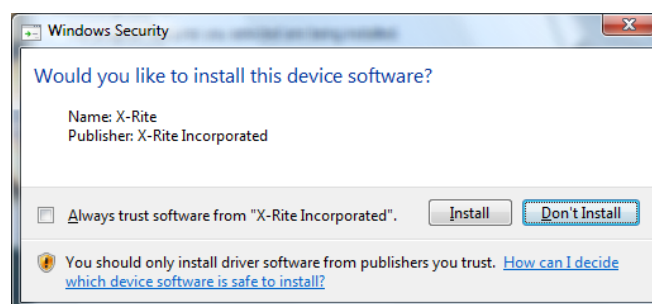


- 10.** The “Ready to Install the Program” screen appears. Click [Install].

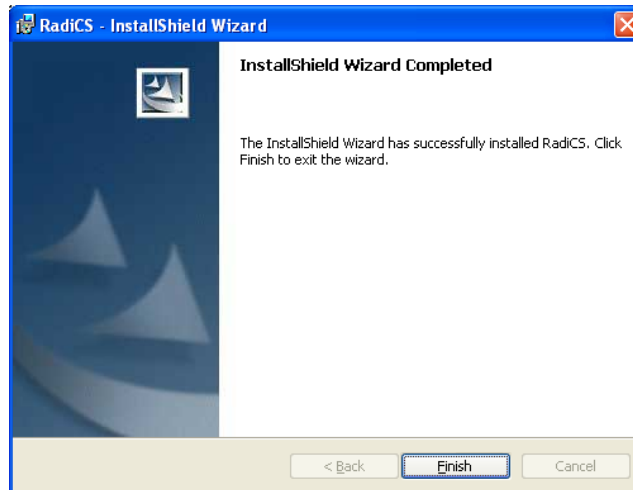
---

**Note**

- For Windows Vista or Windows 7, “Windows Security” screen appears during installation, and you are asked whether to install the device software of “X-Rite”. In that case, click [Install].



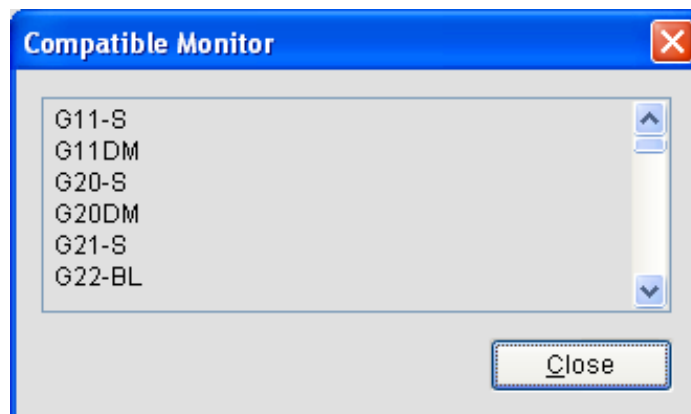
## 11. The “InstallShield Wizard Completed” screen appears. Click [Finish].



---

### Note

- Click the “Compatible Monitor” in the “EIZO RadiCS Setup” screen to see “Compatible Monitor”.  
If the model name of your monitor is not shown there, execute “RadiCS\_MonitorFile\_x.x.x.exe” on the EIZO LCD Utility Disk (CD-ROM) supplied with your monitor.



## 7-8. Installation of RadiCS Network Upgrade Software

### Note

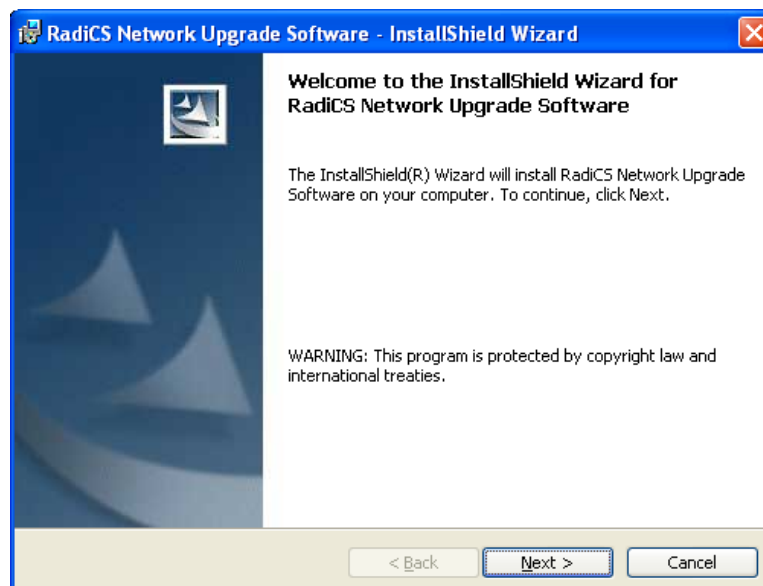
- “.NET Framework 2.0” is installed automatically.

### Procedure

1. Insert the “RadiCS CD-ROM” to the drive.
2. The “EIZO RadiCS Setup” screen appears. Click “Install RadiCS Network Upgrade Software”.

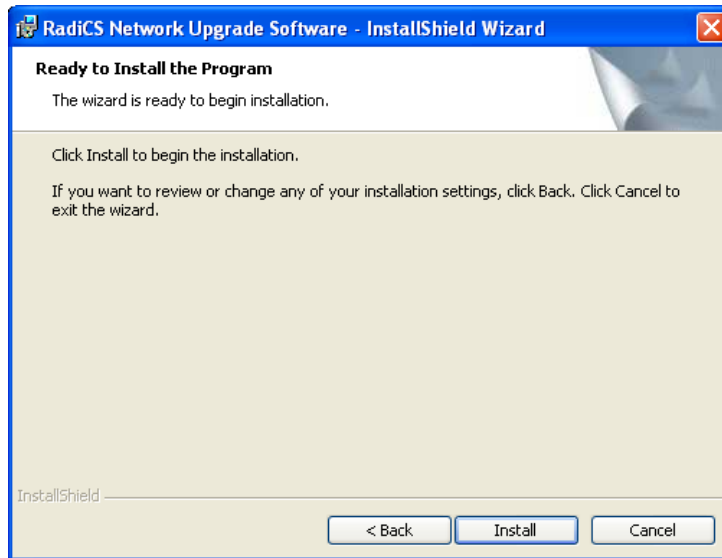


3. The “RadiCS Network Upgrade Software - InstallShield Wizard” screen appears. Click [Next].

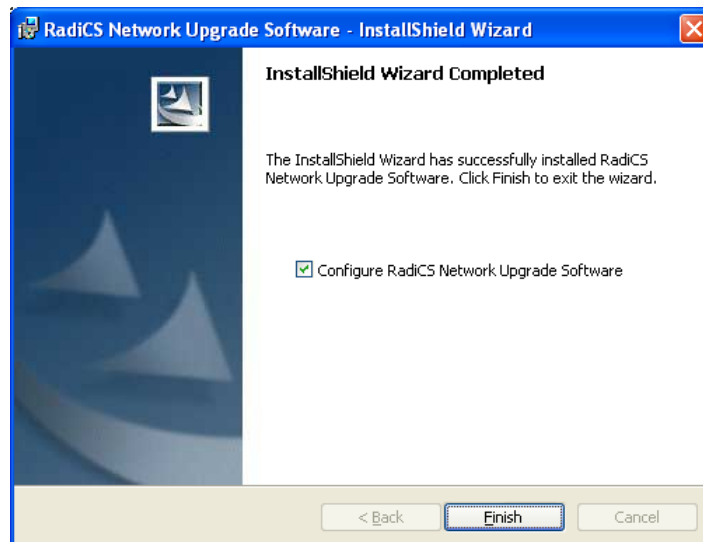




**4. The “Ready to Install the Program” screen appears. Click [Install].**



**5. The “InstallShield Wizard Completed” screen appears. Click [Finish].**



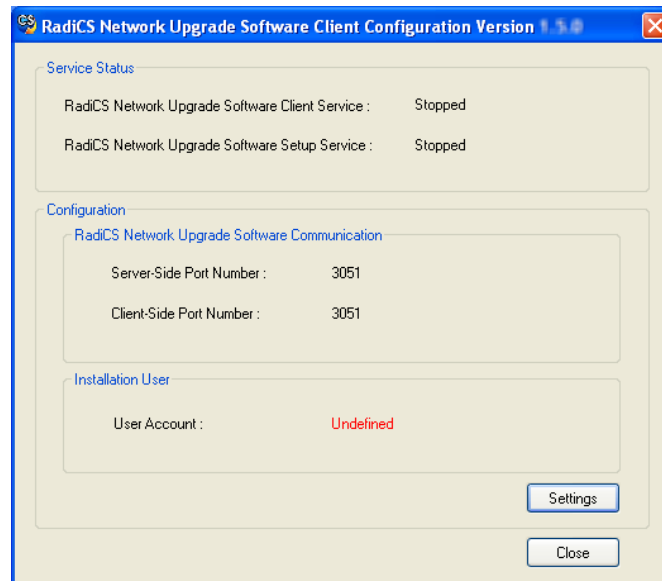
**Attention**

- When “Configure RadiCS Network Upgrade Software” is selected and [Finish] is clicked, “RadiCS Network Upgrade Software Client Configuration” starts.
- “RadiCS Network Upgrade Software Client Configuration” can be started from [Start] - [All Programs] - [EIZO] - [RadiCS Network Upgrade Software Client Configuration] in Windows.

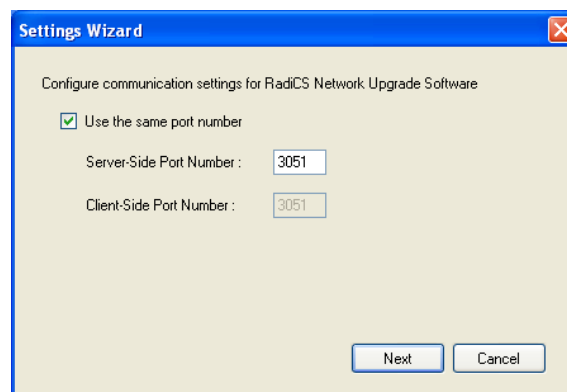
## 7-9. Configuring RadiCS Network Upgrade Software

### Procedure

1. Either continue from “7-8. Installation of RadiCS Network Upgrade Software” (page 104) to perform the settings, or click [Start] - [All Programs] - [EIZO] - [RadiCS Network Upgrade Software Client Configuration] in Windows.
2. The “RadiCS Network Upgrade Software Client Configuration” screen appears. Click [Settings].

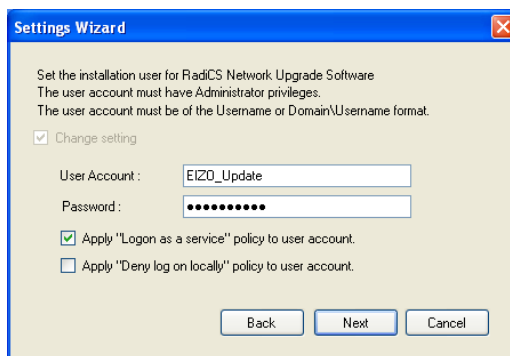


3. The “Settings Wizard” screen appears. If the change of communication port is required, set the following and click [Next]. If the change of communication port is not required, click [Next].
  - Use the same port number: Select this to use the same port number for the RadiNET Pro server / Gateway computer (RadiCS Network Upgrade Software Server) and RadiCS computer (RadiCS Network Upgrade Software Client). (This is the default setting)
  - Server-Side Port Number: Set the port number for the RadiCS Network Upgrade Software
  - Client-Side Port Number: Set the port number for the RadiCS Network Upgrade Software Client. When [Use the same port number] is selected, the same port number as [Server-Side Port Number] is used



#### 4. The setting screen of user for RadiCS Network Upgrade Software Service appears. Set the following and click [Next].

- User Account: Enter the user name created in “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71).
- Password: Enter password of the user entered in User Account
- Apply “Logon as a service” policy to user account: When using user account in Local, select this. When using user account in Domain, unselect this
- Apply “Deny log on locally” policy to user account: When using a user account in Domain, unselect this. Select only when using a user account in Local and when that user is an exclusive RadiCS network upgrade user.

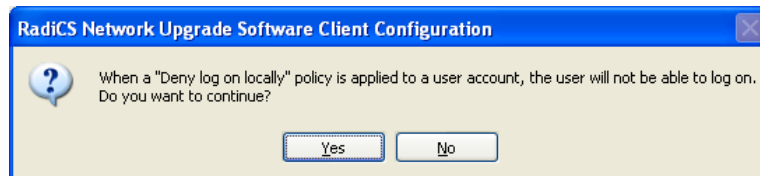


#### Attention

- If “Apply “Deny log on locally” policy to user account” is selected, logging on with that account will no longer be possible.

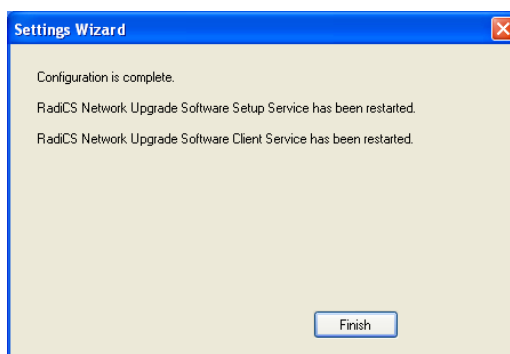
#### Note

- If you select “Apply “Deny log on locally” policy to user account” and then click [Next], the confirmation screen appears. Click [Yes].



- If “Apply “Logon as a service” policy to user account” is selected, the user entered in User Account is added to the local security policy of “Local Policies” - “User Rights Assignment” - “Log on as a service”.
- If “Apply “Deny log on locally” policy to user account” is selected, the user entered in User Account is added to “Local Policies” - “User Rights Assignment” - “Deny log on locally” of the local security policy.

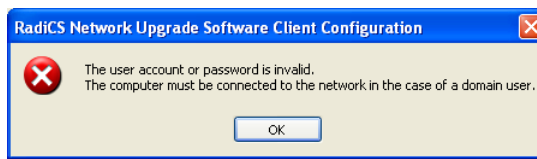
#### 5. The “Configuration is complete.” screen appears. Click [Finish].



---

**Note**

- The error message is displayed if “User Account” or “Password” is invalid. Enter the correct “User Account” or “Password” again.



- The information about security policy is in [“6-6. Configuring the Local Security Policy”](#) (page 54).
  - When set the user for the RadiCS Network Upgrade Software service manually, refer to [“7-11. Setting a user account for RadiCS Network Upgrade Software service”](#) (page 112).
-

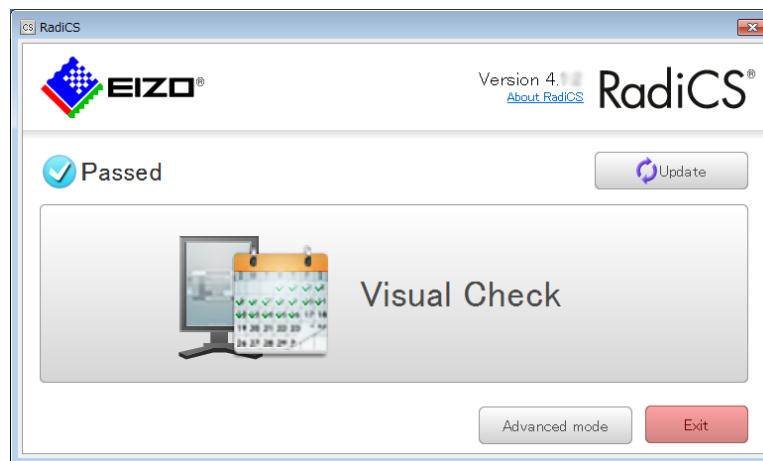
## 7-10. Connecting to RadiNET Pro Server

### Attention

- Although a “connection error” occurs after the following settings in an environment where RadiNET Pro is not running, this does not affect the operation. Once RadiNET Pro starts running, the connection will be established (excluding RadiNET Pro Web Hosting).
- A security system on the network may restrict the communications. In that case, it must be configured so that the communications are enabled.
- RadiNET Pro :  
Two-way communications must be enabled between the RadiNET Pro server and the RadiCS computer.
- RadiNET Pro Enterprise / RadiNET Pro Web Hosting :  
Communications must be enabled between the Enterprise Server, Gateway computer, and RadiCS computer..

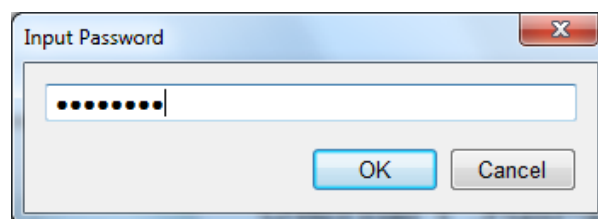
### Procedure

1. Click [Start] - [All Programs] - [EIZO] - [RadiCS] to start RadiCS. Click [Advanced mode]

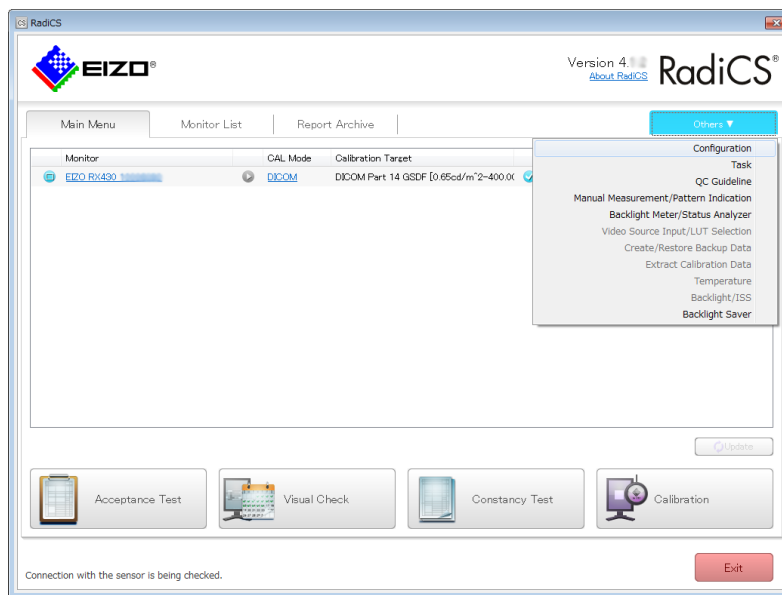


2. The “Input Password” screen appears. Enter the password and then click [OK].

If the password is not changed during RadiCS installation, the password is “password”.



**3. “Advanced mode” starts up. Click [Other] tab and click [Configuration] in the list.**



**4. The “Configuration” screen appears. Click “RadiNET Pro”. Configure the following settings and then click [OK].**

- Select “Use RadiNET Pro”
- RadiNET Pro Server Address: Enter the address of RadiNET Pro server<sup>\*1</sup>
- Server-Side Port Number: Set the port number for the RadiNET Pro server<sup>\*2</sup>
- Client-Side Port Number: Set the port number for the RadiCS.

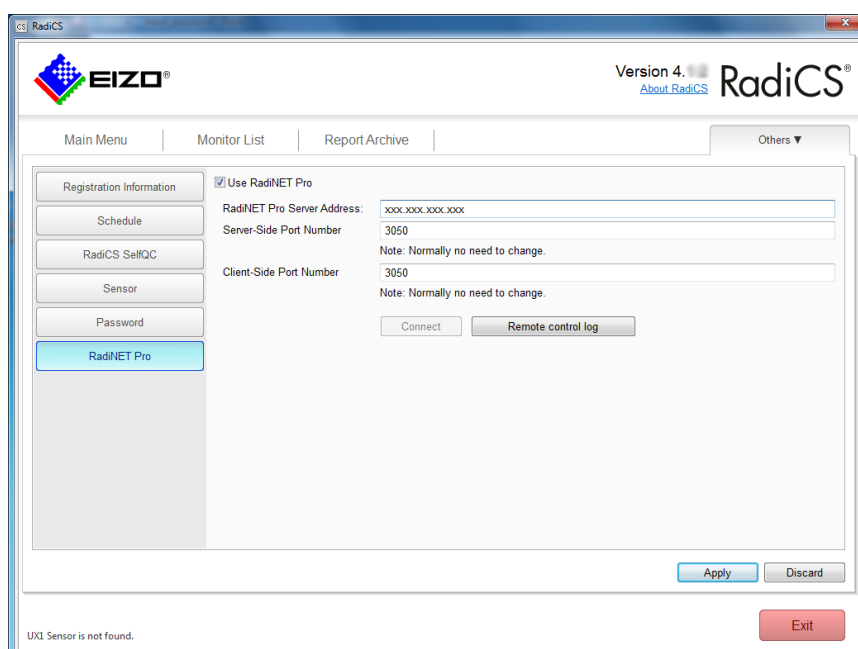
**Attention**

- The port number setting should match the setting of RadiNET Pro.<sup>\*3</sup>

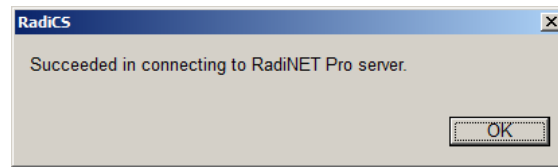
<sup>\*1</sup> For RadiNET Enterprise / RadiNET Pro Web Hosting, enter the address of Gateway computer.

<sup>\*2</sup> For RadiNET Enterprise / RadiNET Pro Web Hosting, set the port number for the Gateway computer.

<sup>\*3</sup> For RadiNET Enterprise / RadiNET Pro Web Hosting, the port number setting should match the setting of Gateway computer.



- 5.** When the connection completed successfully, “Succeeded in connecting to RadiNET Pro server.” message is displayed.



## 7-11. Setting a user account for RadiCS Network Upgrade Software service

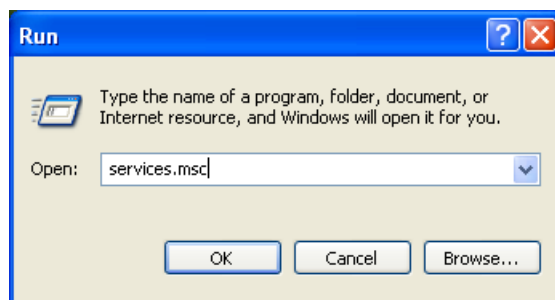
Set the user account for RadiCS Network Upgrade Software Service.

### Attention

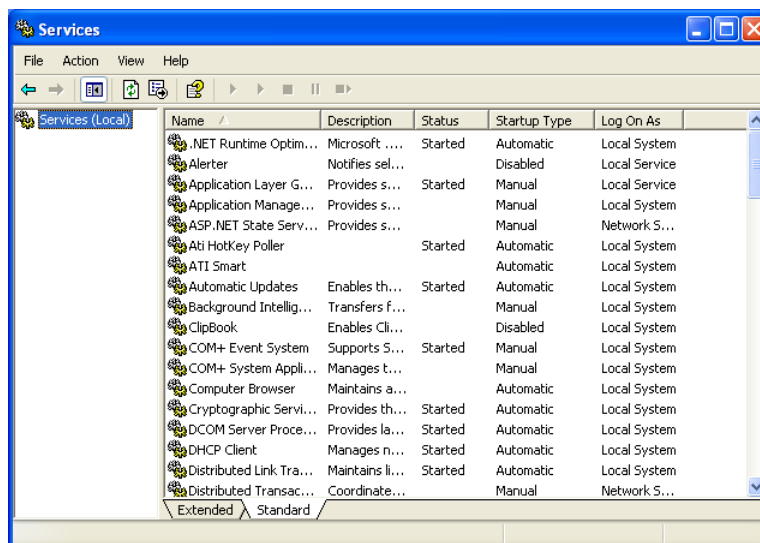
- These settings are made automatically as part of “RadiCS Network Upgrade Software Client Configuration”. If you need to make settings directly, follow the procedure below.

### Procedure

1. Click [Start] - [Run...] in Windows. Enter “services.msc” to “Open:” and then click [OK].

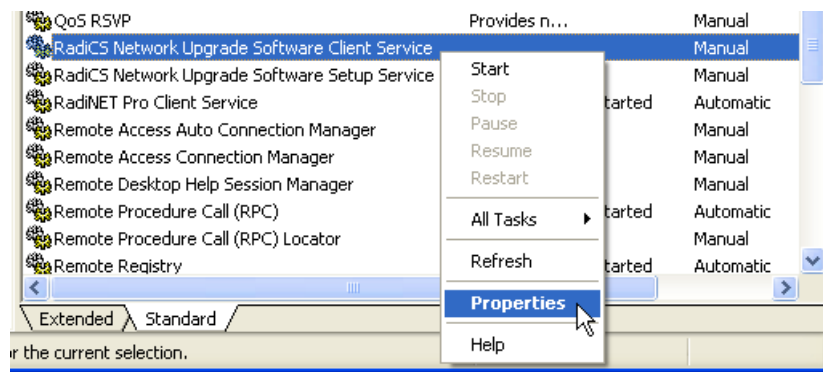


2. The “Services” screen appears. The service list is displayed on the right side of the screen.

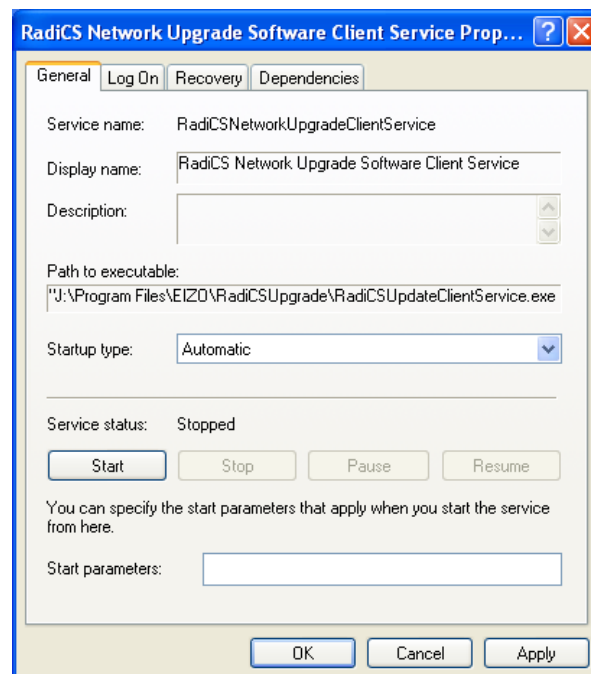




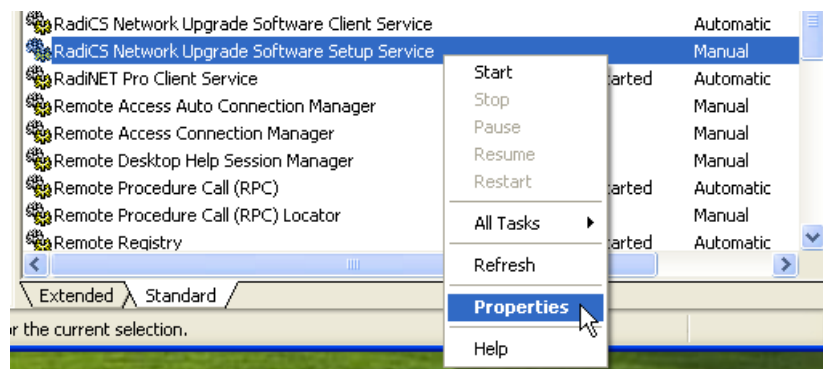
- 3. Click the right mouse button on “RadiCS Network Upgrade Software Client Service” and select [Properties].**



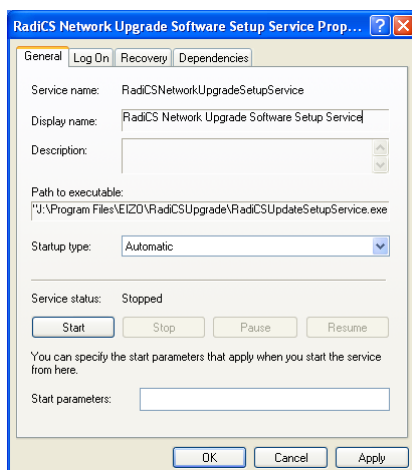
- 4. The “RadiCS Network Upgrade Software Client Service Properties” screen appears. Select “Automatic” in “Startup type” of “General” tab. After entering the information, click [OK].**



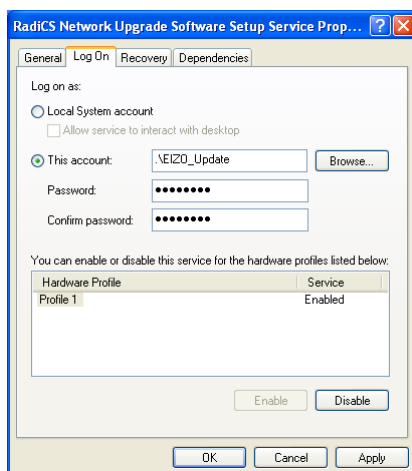
- 5. Click the right mouse button on “RadiCS Network Upgrade Software Setup Service” and select [Properties].**



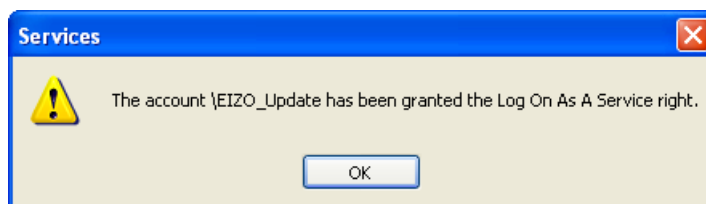
- 6.** The “RadiCS Network Upgrade Software Setup Service Properties” screen appears. Select “Automatic” in “Startup type” of “General” tab. After entering the information, select “Logon” tab.



- 7.** Select “This account” in “Log on as:” of “Log On” tab. Set the following and then click [OK].
- This account: Enter the user name created in “6-2. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 42) or “7-3. Creating a User Account for RadiCS Network Upgrade Software Setup Service” (page 71)
  - Password: Enter password for the account
  - Confirm password: Enter password same as “Password”



- 8.** The message “The account xxxxxx has been granted the Log On As A Service right.” is displayed. Click [OK].



# MAINTENANCE

# Chapter 8 Management of Gateway Computer

## 8-1. Changing the Number of Simultaneous Connections

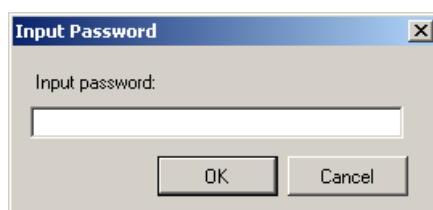
The RadiNET Pro Gateway has a restriction on the number of simultaneous connections from RadiCS computers. This section describes how to change the number of simultaneous connections.

### Attention

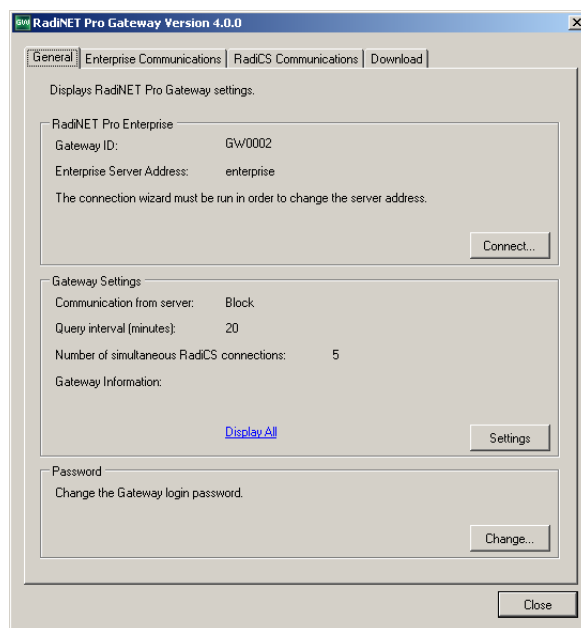
- If you increase the number of simultaneous connections, the time required for remote operations from RadiCS computers will become shorter. However, as you can only specify as many simultaneous connections as you have Windows Server CALs, please check how many CALs you have.
- The minimum number of simultaneous connections is “5”, and the maximum number is “20”.

### Procedure

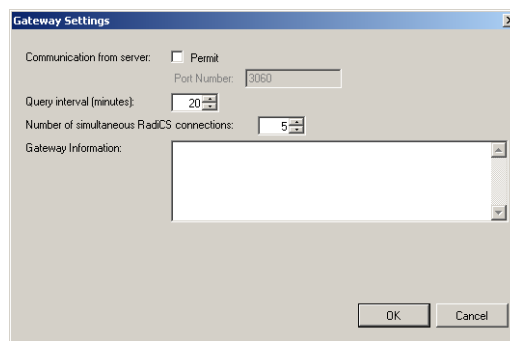
1. Click [Start] - [All Programs] - [EIZO] - [RadiNET Pro Gateway] in Windows.
2. The “Input Password” screen appears. Enter the password and then click [OK].



3. The “RadiNET Pro Gateway” screen appears. Select “General” tab, and then click [Settings] in “Gateway Settings”.



- 4.** The “Gateway Settings” screen appears. Set “Number of simultaneous RadiCS connections:” and click [OK].



## 8-2. How to Change Gateway Computers

This section describes how to take over the settings of the previous Gateway computer when changing the previous Gateway to the new one because of the failure.

### Attention

- When the settings of the previous Gateway computer are not taken over, the monitor removed from previous Gateway computer to new one is considered as the different monitor from the previous one. Therefore, past management history is not integrated.

### Procedure

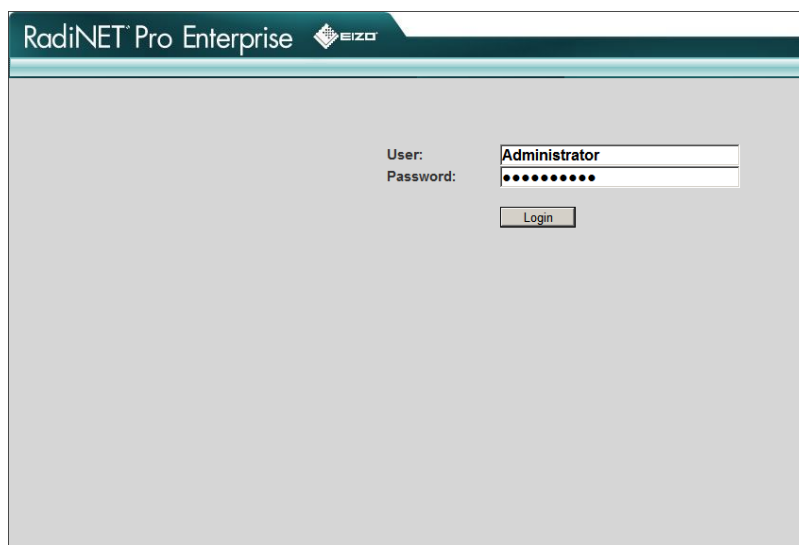
#### 1. Run Internet Explorer on the administrator computer.

#### 2. Access the relevant URL.

- For RadiNET Pro Enterprise : “https://[domain name]/RadiNETPro/”.
- For RadiNET Pro Web Hosting : URL shown on the registration card

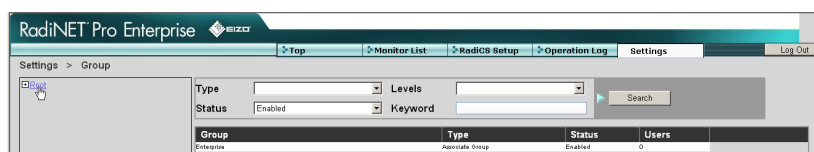
#### 3. The login screen appears. Enter the relevant username and password and click [Login].

- For RadiNET Pro Enterprise  
User : Administrator  
Password : Password00
- For RadiNET Pro Web Hosting  
Username and password shown on the registration card

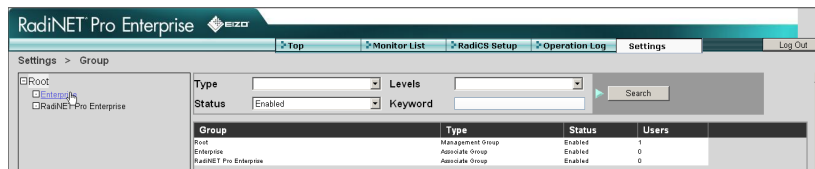


#### 4. The “Top page” screen appears. Select “Group” from “Settings” tab.

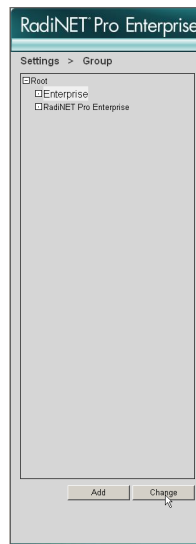
#### 5. The “Settings > Group” screen appears. From the left side of the screen, click “+” at left of “Root”.



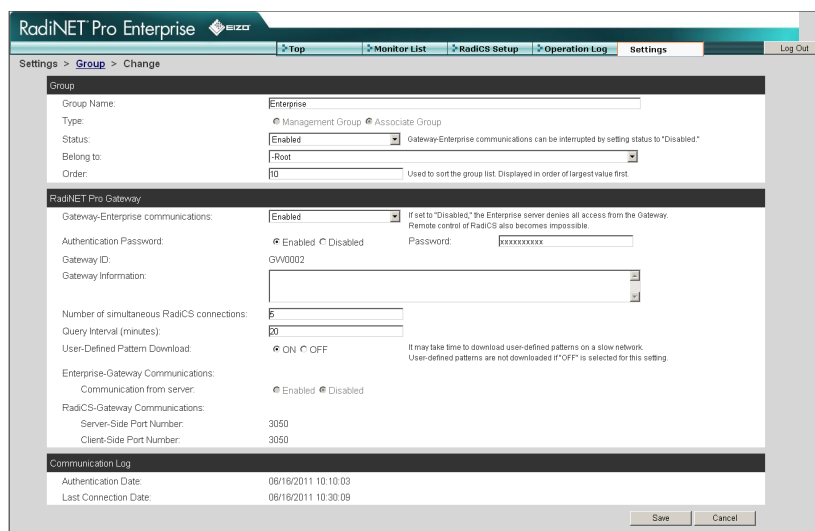
**6. From the left side of the screen, click the group to set.**



**7. Click [Change].**



**8. The “Settings > Group > Change” screen appears. Check “Enabled” of “Authentication Password:”, and then click [Save].**



### Attention

- When creating the associate group with the authentication password of the management group, the “Authentication Password” of the created associate group will be blank. In order to allow settings to be inherited, enter an appropriate password for the associated group.

The screenshot shows the 'RadiNET Pro Enterprise' web interface. The top navigation bar includes 'Top', 'Monitor List', 'RadICS Setup', 'Operation Log', 'Settings', and 'Log Out'. The main content area is titled 'Settings > Group > Change'. It contains two main sections: 'Group' and 'RadINET Pro Gateway'. The 'Group' section has fields for 'Group Name' (Enterprise), 'Type' (Management Group / Associate Group), 'Status' (Enabled), 'Belong to' (-Root), and 'Order' (10). The 'RadINET Pro Gateway' section includes 'Gateway-Enterprise communications' (Enabled), 'Authentication Password' (Enabled / Disabled), 'Gateway ID' (GW0002), 'Gateway Information' (a dropdown menu), 'Number of simultaneous RadICS connections' (5), 'Query Interval (minutes)' (10), 'User-Defined Pattern Download' (ON / OFF), 'Enterprise-Gateway Communications' (Communication from server: Enabled / Disabled), 'RadICS-Gateway Communications' (Server-Side Port Number: 3050, Client-Side Port Number: 3050), and a 'Communication Log' table with columns for 'Authentication Date' and 'Last Connection Date'. The 'Save' and 'Cancel' buttons are at the bottom right.

## 9. Install RadiNET Pro Gateway according to “Chapter 5 Setup of Gateway Computer” (page 15).



# Chapter 9 About Log

## 9-1. Remote Operation Log of Enterprise Server

From the administrator computer using the management console, you can check the history that RadiCS computer or monitor have been remote operated.

### Procedure

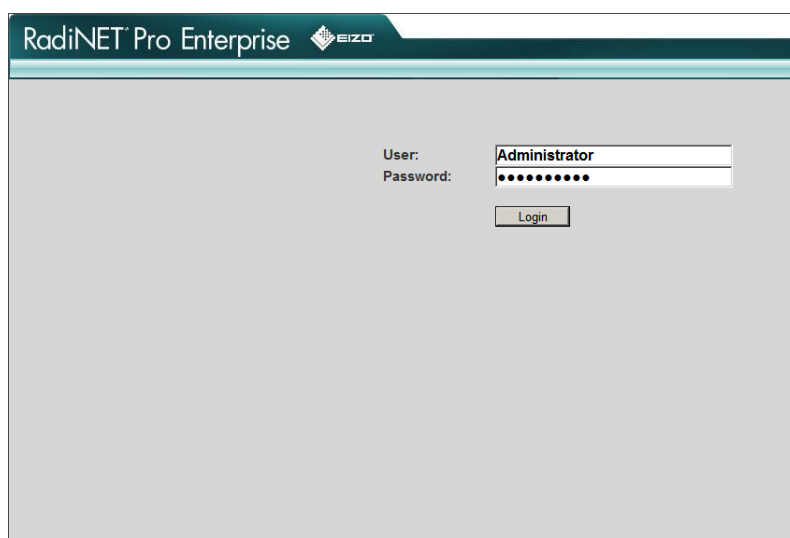
#### 1. Run Internet Explorer on the administrator computer.

#### 2. Access the relevant URL.

- For RadiNET Pro Enterprise : “https://[domain name]/RadiNETPro/”.
- For RadiNET Pro Web Hosting : URL shown on the registration card

#### 3. The login screen appears. Enter the relevant username and password and click [Login].

- For RadiNET Pro Enterprise  
User : Administrator  
Password : Password00
- For RadiNET Pro Web Hosting  
Username and password shown on the registration card



#### 4. Select “Operation Log” tab.



#### 5. The operation log is displayed.

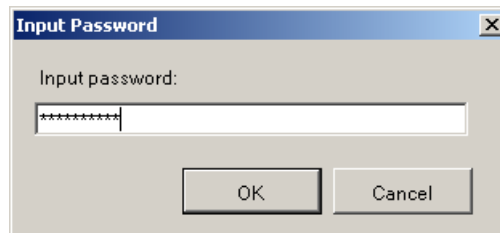
No.▼	Date & Time	User	Operation	Status
7	03/19/2008 02:42	Administrator-B	Log Out	-
6	03/19/2008 02:41	Administrator-B	Calibration(Backlight Sensor)	Completed
5	03/19/2008 02:41	Administrator-B	Login	-

## 9-2. Remote Operation Log of Gateway Computer

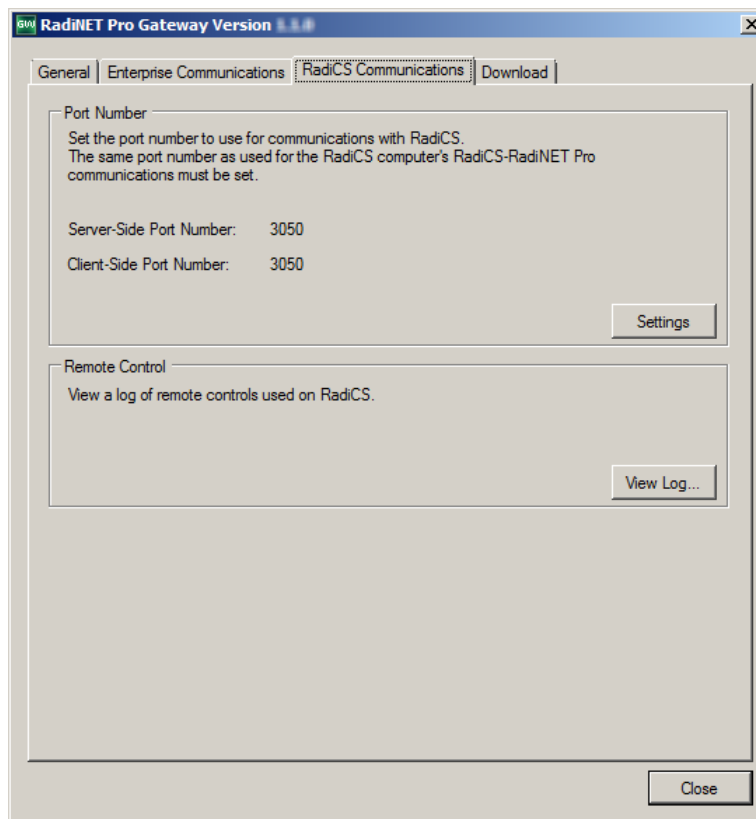
Gateway computer relays the remote operations from Enterprise server to RadiCS computer. You can check the history of the relayed remote operations on Gateway computer.

### Procedure

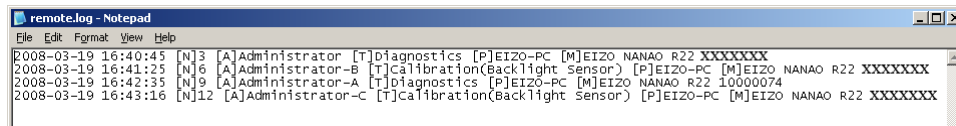
1. Click [Start] - [All Programs] - [EIZO] - [RadiNET Pro Gateway] in Windows on the Gateway computer.
2. The “Input Password” screen appears. Enter the password and then click [OK].



3. Click [View Log...] of “RadiCS Communications” tab.



## 4. “remote.log” file is opened.



ex.

When the log is “2008-03-18\_17:52:00\_[N]3\_[A]Administrator\_[T]Diagnostics\_[P]EIZO-PC [M]EIZO NANA0 R22 xxxxxxxx”

### Meaning

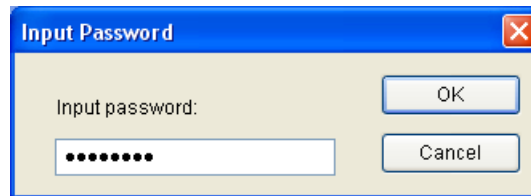
- Execution date and time: 2008-03-18 17:52:00
- Log number [N]: 3
- Tester [A]: Administrator
- Contents of the operation [T]: Self-diagnostic (Diagnostics)
- Name of RadiCS computer [P]: EIZO-PC
- Monitor [M]: EIZO NANA0 R22 xxxxxxxx

## 9-3. Remote Operation Log of RadiCS Computer

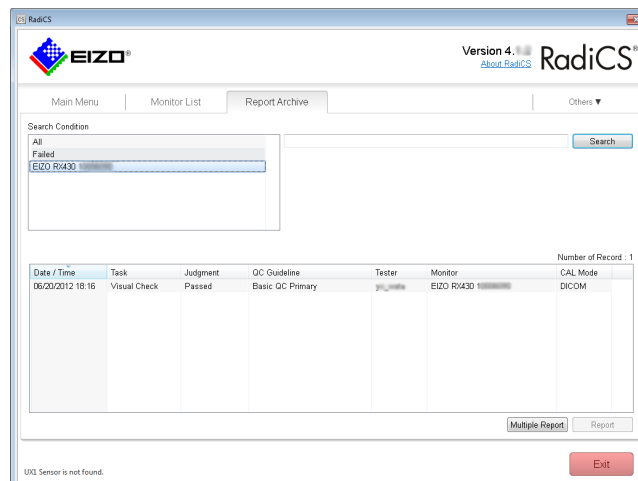
You can check the history of operations performed to RadiCS computer or monitor.

### Procedure

1. On RadiCS computer, click [Start] - [All Programs] - [EIZO] - [RadiCS] in Windows to start. Click [Advanced Mode]
2. The “Input Password” screen appears. Enter the password and then click [OK].



3. “Advanced Mode” starts up. Click “Report Archive” tab. The operation history appears.



## 9-4. About Other Logs

---

### ● System Log of Enterprise Server

---

**Attention**

- Logs cannot be viewed in RadiNET Pro Web Hosting.
- 

Log data of Enterprise server is saved in the RadiNET Pro Enterprise install folder of the Enterprise server.  
ex.) The file is created in “C:\Program Files\EIZO\RadiNET Pro\syslog\”.

### ● System Log of Gateway Computer

Log data of Gateway server is saved in the RadiNET Pro Gateway install folder of the Gateway server.  
ex.) The file is created in “C:\Program Files\EIZO\RadiNETProGW\syslog\”.

### ● Error Log of RadiCS Computer

In the event of the RadiCS failure, error log file (radics.log) is created.  
ex.) The file is created in “C:\Program Files\EIZO\RadiCS4\RadiCS\log\radics.log”.

# REFERENCE

# Chapter 10 About Security

Enterprise server and Gateway computer are connected to the Internet. Therefore, those are exposed to the various threats. For the secure communication, RadiNET Pro Enterprise and RadiNET Pro Gateway have various security functions. This section describes the security of this system.

## 10-1. Security of the System

This system has the following security functions.

- Identification and authentication of user
- Identification and authentication of device
- Securing of communication path
- Collection of remote operation log

## 10-2. Identification and Authentication of User

### Authentication with User Name and Password

- To perform various operations with the management console, the authentication with user name and password is required. When the user name or password is leaked, the impact can be limited because the manageable range of each user is restricted.
- The user can only access the data of the group which it belongs to and its subordinate groups. Dividing users to “Administrator”, “User” and “Read-only user” can define the range of accessible data.

## 10-3. Identification and Authentication of Device

### Authentication of the Password for RadiNET Pro Gateway

After setting the authentication password published by Enterprise server at the first setting, Gateway computer can access Enterprise server. The authentication password becomes disabled after Enterprise server authenticates the Gateway computer. Therefore, even if the authentication password is leaked, Enterprise server does not authenticate the Gateway computer that uses the password. However, the authentication password set to the management group remains enabled unless disabled by the user. Disable the password on completion of the authentication for Gateway computer.

## 10-4. Securing of Communication Path

### SSL Communication

SSL is used for the communication between Enterprise server and Gateway computer. By using SSL, the leakage and falsifying of information are prevented.

## 10-5. Recording Remote Operation Log

### Recording Remote Operation Log on the Server and Computer

Record the remote operation log on Enterprise server, Gateway computer and RadiCS computer. The information about “when”, “who”, “to which computer” and “what is done” is recorded in the log.

## 10-6. Patient Information

### Handling of Patient Information on the Server and Computer

Patient information is not handled on Enterprise server, Gateway computer and RadiCS computer.

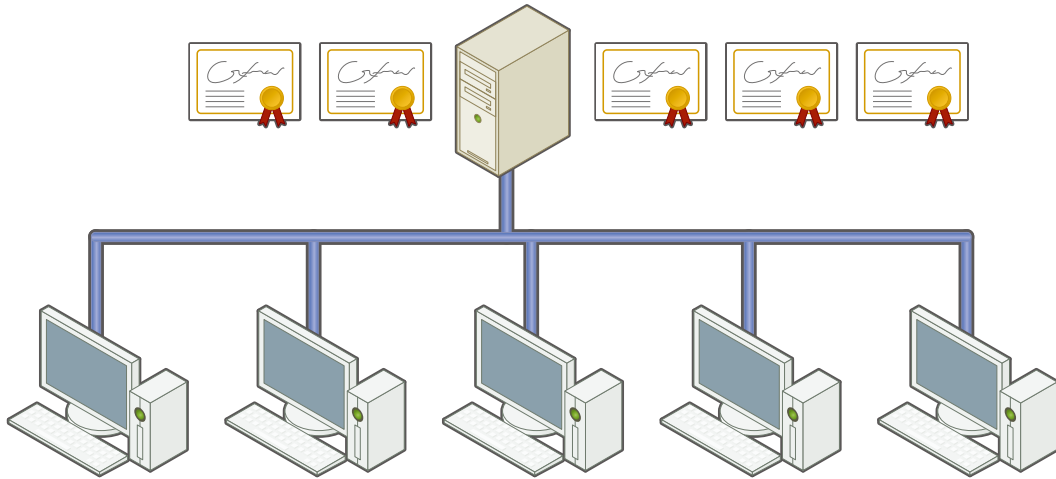


# Chapter 11 About License

## 11-1. License Required for Gateway Computer

- If you are using Windows Server 2003, you need to have Client Access License (CAL).
- If purchasing a new CAL, it is recommended that you use the Per Server Mode to reduce the number of CALs to be purchased. However, the requirements depend on your system configuration so please purchase CALs to suit your system configuration.
- In the environment where you are going to deploy a Gateway computer, if all RadiCS computers have “Device CAL”, there is no need for new Windows Server CAL.
- The Gateway computer has a restriction on the number of simultaneous connections. You need to purchase the same number of Windows Server CALs as the number of simultaneous connections. See [“8-1. Changing the Number of Simultaneous Connections” \(page 116\)](#) for details on how to change the number of simultaneous connections. (The default value for the number of simultaneous connections is five.)

## Per Server Mode

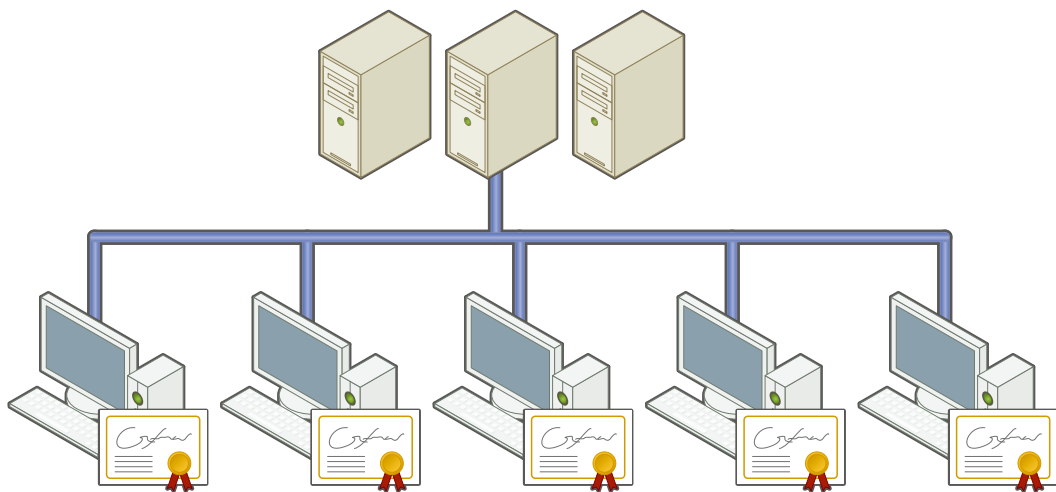


- Windows Server comes with Windows Server CAL. The number of CALs determines the number of devices or users that can access it simultaneously.

ex.)

If Windows Server comes with five Windows Server CALs, then five clients can be used to access it. The 6th client cannot access Windows Server until one of the five clients is disconnected.

## Per Device Mode



- When using the client computer to which installed Windows Server CAL, any number of users can access Windows Server. Also, multiple Windows Servers can be accessed.

# 11-2. License Required for SQL Server

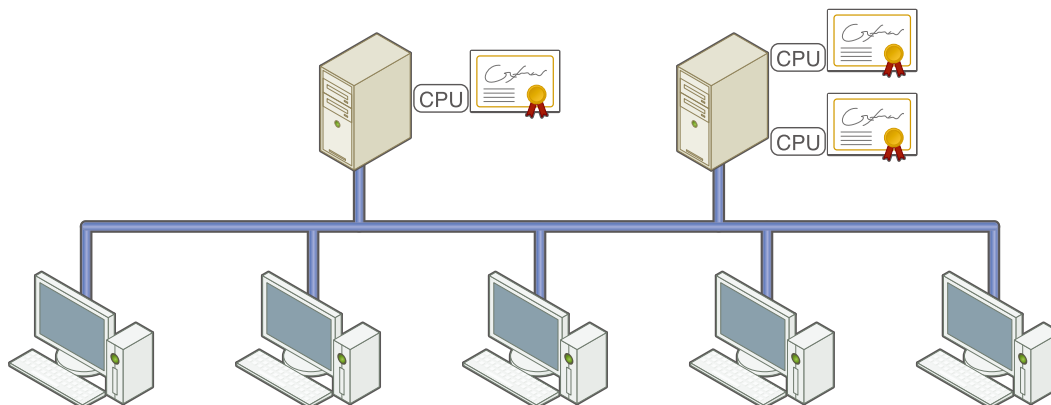
**Attention**

- A license is not required for RadiNET Pro Web Hosting.
- You need to have a license in accordance with Microsoft licensing in order to use SQL Server. Please obtain the correct license for your system configuration.
- The RadiNET Pro Enterprise system has a restriction on the number of simultaneous connections. You need to purchase the same number of SQL Server CALs as the number of simultaneous connections. See “8-1. Changing the Number of Simultaneous Connections” (page 116) for details on how to change the number of simultaneous connections. (The default value for the number of simultaneous connections is five.)
- You cannot use User CAL in RadiNET Pro Enterprise system.

Processor license	<ul style="list-style-type: none"><li>• The number of licenses required is the same number of CPUs on the server to which SQL Server is installed.</li><li>• Multi-core CPUs are treated as a single CPU.</li><li>• The licenses are independent of the number of Gateway computers.</li></ul>
Server / CAL license	<p>Device CAL (Client Access License)</p> <ul style="list-style-type: none"><li>• A “server license” is required for the server on which SQL Server is installed.</li><li>• Gateway computers that use the server on which SQL Server is installed require a “device CAL”.</li><li>• Gateway computers with a “device CAL” can utilize multiple different servers with SQL Server installed.</li><li>• Depending on the number of Gateway computers, this option may be cheaper than a “processor license”.</li></ul>

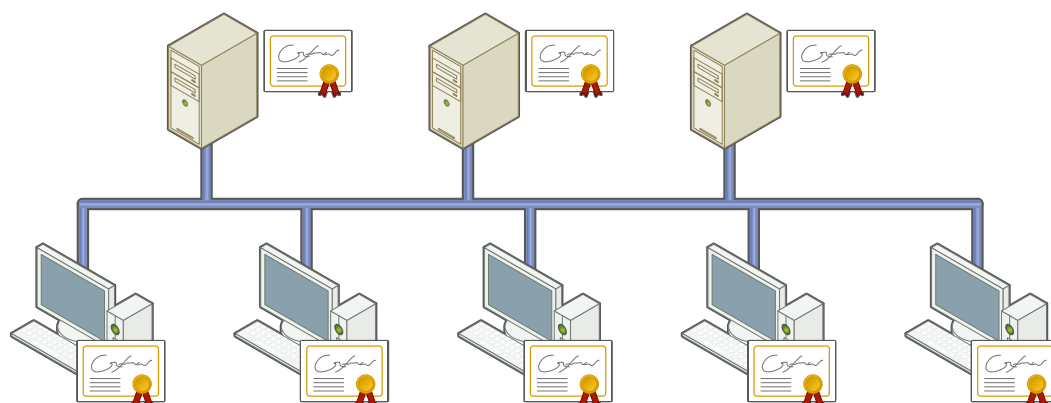
Difference between SQL Server CAL and SQL Server Workgroup Edition CAL	
SQL Server CAL	Can connect regardless of edition.
SQL Server Workgroup Edition CAL	Can only connect to Workgroup Edition.

## Processor License



- A processor license is required for each CPU on the server on which SQL Server is installed.
- As the above system has three CPUs, three processor licenses are required.

## Server / CAL License “Device CAL”



- A “server license” is required for the server on which SQL Server is installed.
- Client computers that use the server on which SQL Server is installed require a “device CAL”.
- Client computers with a “device CAL” can utilize multiple different servers with SQL Server installed.

## Chapter 12 Other Settings

### 12-1. Moving Monitors between Groups

RadiNET Pro Enterprise identifies the medical imaging display monitor with the following: Gateway computer that the monitor belongs to, manufacturer, model, and serial number. When the monitor is moved from the Gateway computer that the monitor currently belongs to (called previous Gateway computer) to the other Gateway computer (called new Gateway computer), the monitor that belongs to the new Gateway computer is considered the different monitor from the one that had belonged to the previous Gateway computer. Therefore, the monitor management history on the previous Gateway computer is not taken over. To take over the management history, refer to [“8-2. How to Change Gateway Computers” \(page 118\)](#).

## 12-2. Access Restriction to Management Console

### Attention

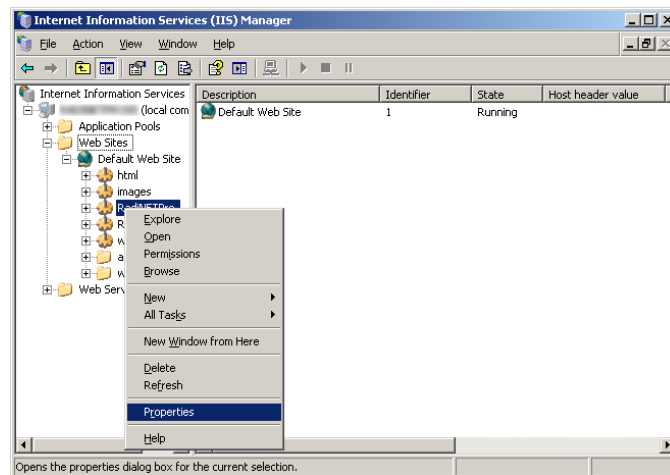
- These settings are not required for RadiNET Pro Web Hosting.

To restrict the computer access to the management console, set the authentication. However, the client certificate published by the certification authority is required to the setting.

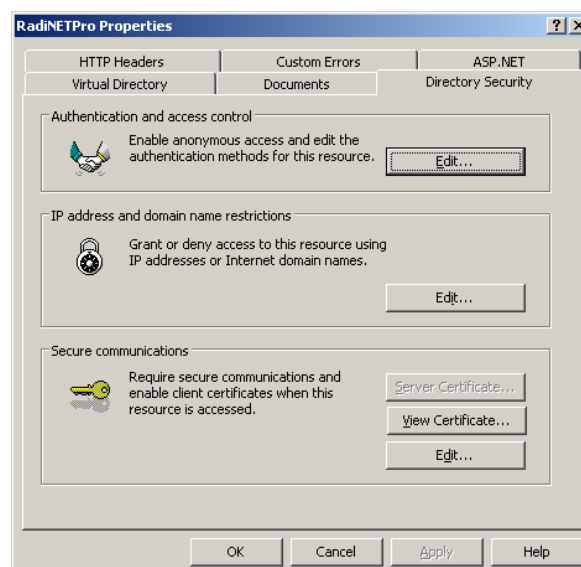
### ● For Windows Server 2003

#### Procedure

1. On Enterprise server, select [Start] - [Administrative Tools] - [Internet Information Services (IIS) Manager] in Windows.
2. The “Internet Information Services (IIS) Manager” screen appears. Select “Web Sites” - “Default Web Site” - “RadiNETPro”. Click the right mouse button and select [Properties] from the menu.



3. The “RadiNETPro Properties” screen appears. Select “Directory Security” tab and click [Edit...] of “Secure communications”.

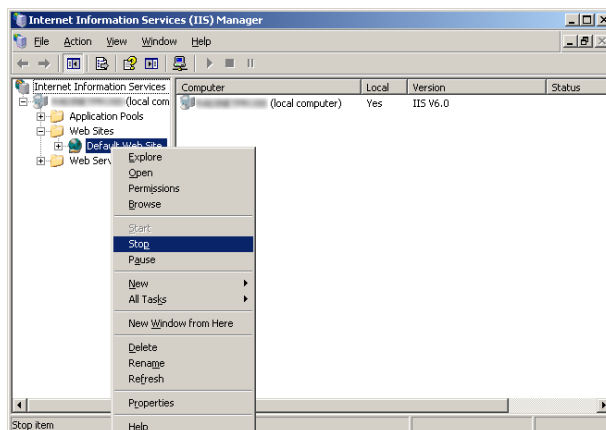


4. The “Secure Communications” screen appears. Check “Require client certificates” checkbox, and click [OK].

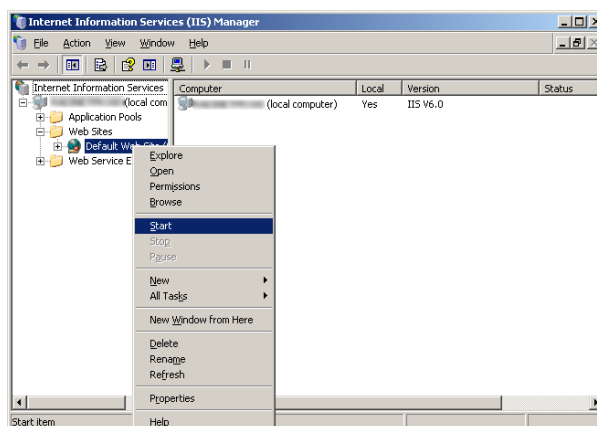


5. The “RadiNETPro Properties” screen reappears. Click [OK].

6. The “Internet Information Services (IIS) Manager” screen reappears. Click the right mouse button on “Default Web Site” and select [Stop] from the menu.



7. Click the right mouse button on “Default Web Site” again, and select [Start] from the menu.



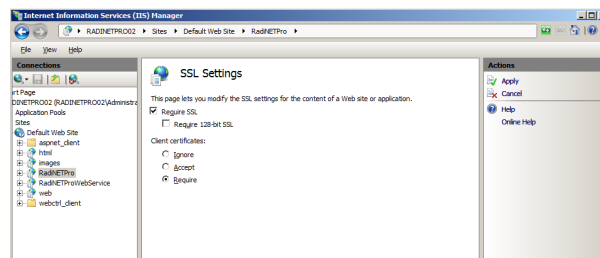
**Attention**

- Install the client certificate on the administrator computer.

## ● For Windows Server 2008

### Procedure

1. On Enterprise server, select [Start] - [Administrative Tools] - [Internet Information Services (IIS) Manager] in Windows.
2. The “Internet Information Services (IIS) Manager” screen appears. Click [(RadiNET Pro server name)] - [Sites] - [Default Web Site] - [RadiNETPro].
3. The “RadiNETPro Home” screen appears. Click [SSL Settings].
4. The “SSL Settings” screen appears. Check [Require] of “Client certificates:”. From the right side of the screen, Click [Apply].



5. Select [(RadiNET Pro server name)] on the left side of the screen and then click [Restart] on the right side of the screen.



# Chapter 13 Adding monitors

This chapter describes the procedures to add the monitors.

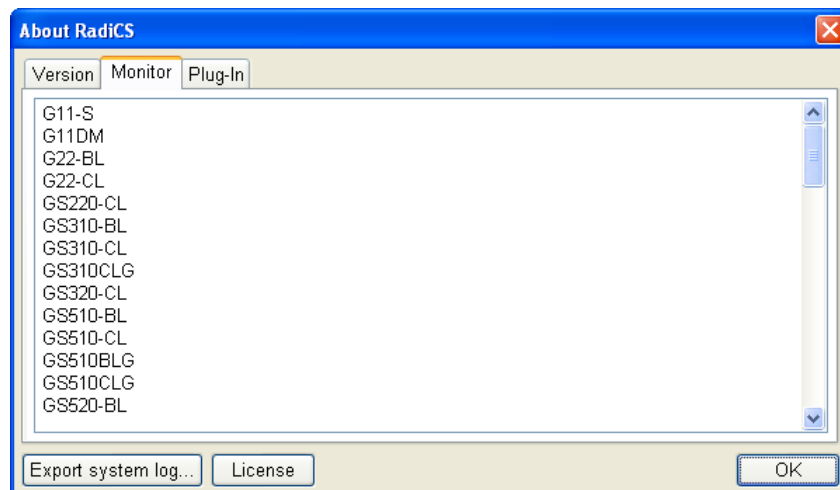
## 13-1. Procedures on RadiCS Computer

### Procedure

1. Click [Start] - [All Programs] - [EIZO] - [RadiCS] to start RadiCS.
2. Click “About RadiCS”.



3. The “About RadiCS” screen appears. Click “Monitor” tab. Confirm that a model name of the monitor you want to add is shown on the list. If not, go on to step 4. (When your model name is shown, the following steps are not necessary.)



4. Insert the EIZO LCD Utility Disk (CD-ROM) supplied with added monitor to the drive of RadiCS computer.
5. Double click “RadiCS\_MonitorFile\_x.x.x.exe” file on the EIZO LCD Utility Disk (CD-ROM) to execute it.

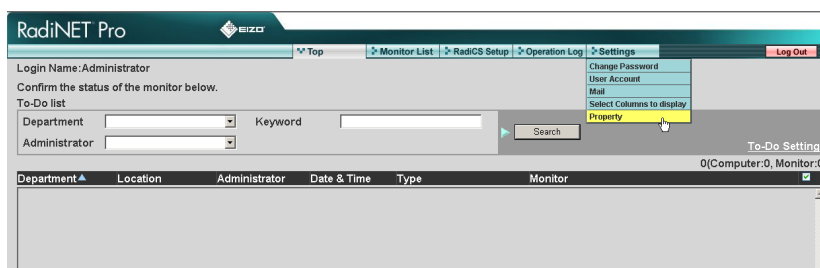
## 13-2. Procedures on RadiNET Pro Server

### Attention

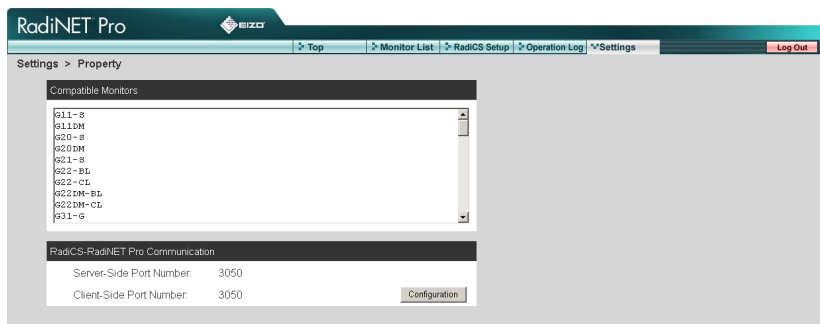
- These settings are not required for RadiNET Pro Web Hosting.

### Procedure

1. From the administrator computer, access the RadiNET Pro management console.
2. The “Login” screen appears. Login with a user account with administrator authority (“Administrator”).
3. The top page appears. From the menu bar, click “Settings” - “Properties”.



4. The “Settings > Property” screen appears. Confirm that a model name of the monitor you want to add is shown on the list. If not, go on to step 5. (When your model name is shown, the following steps are not necessary.)



5. Insert the EIZO LCD Utility Disk (CD-ROM) supplied with added monitor to the drive of RadiNET Pro server.
6. Double click “RadiCS\_MonitorFile\_x.x.x.exe” file on the EIZO LCD Utility Disk (CD-ROM) to execute it.



EIZO NANAO CORPORATION

<http://www.eizo.com>

Copyright © 2012 EIZO NANAO CORPORATION All rights reserved.

5th Edition-November, 2012

03V23930E1  
(U.M-WEBHOSTING)